GESTIÓ DE LA CONFIANÇA EN INFRAESTRUCTURES DE CLAU PÚBLICA (PKI)

Memòria del projecte de final de carrera corresponent als estudis d'Enginyeria Superior en Informàtica presentat per Jordi Gaya Sans i dirigit per Helena Rifà Pous.

Bellaterra, setembre de 2009

El firmant, Helena Rifà Pous , professor del Departament d'Enginyeria de la Informació i de les Comunicacions de la Universitat Autònoma de Barcelona

CERTIFICA:

Que la present memòria ha sigut realitzada sota la seva direcció per Jordi Gaya Sans

Bellaterra, setembre de 2009

Firmat: Helena Rifà Pous

A la meva mare que sempre ha confiat en mi

Agraïments

En primer lloc vull donar les gràcies a la meva directora de projecte, Helena Rifà Pous, per haver invertit cada dijous durant 6 mesos el seu temps, per la seva predisposició en tot moment a resoldre els meus dubtes i pels consells, suggeriments i apreciacions que m'ha fet arribar, sempre amb bon criteri, durant l'elaboració d'aquest projecte.

Gràcies a tots els companys de fatigues i alegries durant aquests involvidables anys.

Finalment gràcies a la meva família pel suport que m'han donat durant tots aquests anys.

Índex

Índex de figures

Índex de taules

Glossari d'Acrònims

API Application Programming Interface

ASN.1 Abstract Syntax Notation One

B2B Business to Business

BCA Bridge Certification Authority

BCP Best Current Practices

BER Basic Encoding Rules

BVA Bridge Validation Authority

CA Certificate Authority

CD Compact Disc

CMP Certificate Management Protocol

CR Certificate Repository

CRL Certificate Revocation List

CSC Cryptographic Smart Card

dEIC departament d'Enginyeria de la Informació i de les Comunicacions

EE End Entity

GNU GNU is Not Unix

GPL GNU General Public License

IDL Interface Definition Language

IETF Internet Engineering Task Force

JCE Java Cryptography Extension

JDK Java Development Kit

JCA Java Cryptography Architecture

JCE Java Cryptography Extension

JS Java Script

JSS Java Security Services

LGPL GNU Lesser General Public License

MD5 Message-Digest Algorithm 5

MPL Mozilla Public License

NSS Network Security Services

OCSP Online Certificate Status Protocol

OID Object IDentifier

OU Unitat Organitzativa

PKI Infraestructures de Clau Pública

PKIX Infraestructures de Clau Pública X.509

PSC Prestador de Serveis de Certificació

QoS Quality of Service

RA Registration Authority

RCA Root Certificate Authority

RFC Request For Comments

SHA Secure Hash Algorithm

TP Trust Provider

TPL Trust Provider Link

URL Uniform Resource Locator

URI Uniform Resource Identifier

VA Validation Authority

X.509v3 Estandard ITU d'extensions de certificació

XML Extensible Markup Language

XPath XML Path Language

XPCOM Cross Platform Component Object Model

XUL XML User Interface Language

Capítol 1

Introducció

Aquest projecte final de carrera s'emmarca dintre de l'àrea temàtica de la certificació digital, que forma part de la criptografia asimètrica , concretament de les Infraestructures de Clau Pública (PKI). Una tecnologia de seguretat que autentica qualsevol transacció, aportant la confiança necessària a les aplicacions de comerç electrònic, i que es troba disponible per qualsevol usuari en qualsevol localització. Una tecnologia de seguretat que no evita totalment el frau, on la seva implementació resulta cara, i que obliga a readaptar a fons el *hardware* i *software* corporatius per ser efectiva. Ambdues descripcions són aplicables a les PKI, però això no impedeix que - amb els seus pros i contres – la seva utilització suposi una gran ajuda allí on es requereixi una forta autenticació, ja es tracti de transaccions Business to Business (B2B), operacions bancàries o comunicacions que impliquin dades personals i privades.

Altrament, la penetració en el mercat global de les aplicacions d'ús general encara no es un fet. L'explicació de la lenta adopció de les solucions basades en PKI és deguda als problemes d'interoperatibitat. La interoperatibitat no es caracteritza simplement en una mera qüestió tecnològica, de fet, és una àmplia gama de qüestions tècniques,jurídiques i polítiques. La indústria de les PKI s'ha ocu-

pat dels problemes referents a la interoperatibitat tècnica a través d'un procés de normalització del tipus de dades i protocols. Avui en dia, tot i la flexibilitat de les especificacions, la tecnologia PKI ha assolit la maduresa i el cumpliment dels objectius bàsics d'interoperatibitat entre els diferents proveïdors. Tanmateix, el gran inconvenient actual per l'adopció de PKI és la dificultat d'implementar una solució delimitada a les diferències jurídico-polítiques de cada país. Els governs són reticents a reconèixer a entitats emissores d'una altra nació, si no prenen part en el control de qualitat i d'altra banda, l'àmbit de responsabilitat d'una entitat emissora de certificació no està clar. Diverses propostes s'han presentat per solventar aquests problemes, com ara l'encreuament de certificats o el pont de certificació. No obstant això, cap d'ells té èxit a causa de la complexitat implicada en la gestió d'aquestes infraestructures i la perspectiva generalista en què es basen.

El present projecte pretén implementar un model de confiança que permeti la integració i la interoperatibitat de les diferents illes de PKI, donant resposta a la necessitat anunciada anteriorment. Aquest nou model considera la confiança una relació particular, una gestió a través d'entitats especialitzades que poden avaluarne els riscos i els processos. Un model basat en llistes de confiança que permet als usuaris una visió personalitzada de confiança sense haver d'involucrar-se en els detalls tècnics. Els usuaris són les entitats finals responsables de l'assignació de confiança dins del seu context. Es proporciona la facilitat d'identificar l'abast i les atribucions de cada autoritat per prendre la decisió més adequada a les necessitats del usuari.

1.1 Objectius

En aquest apartat s'enumeren els objectius que s'han marcat per al desenvolupament del projecte:

1. Implementar un model basat en proveïdors de confiança,amb ús d'ontologies per classificar els atributs de confiança.

2. Anàlisi dels requisits que ha de tenir el nou model que es desenvoluparà.

3. Disseny i construcció d'un joc de proves que permeti avaluar el funcionament i rendiment del nou model.

4. Integrar l'aplicació client en navegadors web.

5. Implementar noves extensions del certificat de PKI segons l'estàndard X.509 (veure [RFC3280]) que permetin automatitzar el procés de gestió de la confiança.

6. Garantir en tot moment la interoperabilitat dels certificats amb les aplicacions actuals.

1.2 Estructura de la Memòria

A continuació es mostra com s'ha estructurat la memòria i s'explica amb una breu descripció el contingut de cada capítol.

- **Capítol 2: Estat de l'art**. En aquest capítol s'explicaran els conceptes previs necessaris per poder contextualitzar el projecte. L'ordre de presentació serà de més general a més concret. S'explicarà què són les PKI, els models existents, com funcionen i un estudi comparatiu. Finalment es presentarà el marc on es desenvoluparà el projecte.

- **Capítol 3: Anàlisi**. En aquest capítol analitzarem els requisits que ha de tindre el nou model de confiança que es vol desenvolupar, així com també un breu estudi de viabilitat i alguns aspectes que caldrà tenir en compte en

les fases de disseny i implementació. Finalment presentarem la planificació temporal prevista de les diferents etapes del projecte.

- **Capítol 4: Disseny**. En aquest capítol s'exposaran les decisions de disseny que s'han pres per complir amb els requisits establerts en el capítol d'anàlisi. Així mateix, s'explicarà detalladament l'arquitectura, que permetrà estructurar la informació que s'intercanvien les diverses entitats.

- **Capítol 5: Implementació**. En aquest capítol s'explicarà com s'ha organitzat el codi a partir del disseny del model que s'ha fet, així com les decisions d'implementació que s'han pres per obtenir un model modular i flexible.

- **Capítol 6: Proves**. En aquest capítol s'explicarà l'entorn on s'han dut a terme els tests del model. Finalment s'analitzaran els resultats obtinguts i se'n farà una interpretació exhaustiva.

Per acabar la memòria s'ha fet un capítol de conclusions on es resumirà la feina feta i s'enumeraran els objectius assolits. Posteriorment s'explicaran les conclusions a les què s'ha arribat en base als resultats obtinguts i es presentaran una sèrie de línies futures de treball. Finalment es farà una valoració personal del projecte.

Capítol 2

Estat de l'art

En aquest capítol s'expliquen els conceptes previs necessaris per poder contextualitzar el projecte. L'ordre de presentació serà de més general a més concret. S'explica què són les PKI, els models existents i com funcionen. Finalment es presenta el marc on es desenvolupa el projecte.

2.1 Conceptes Generals

En aquest apartat es realitza una breu introducció dels conceptes teòrics que engloben les PKI, basades en la criptografia asimètrica i dels elements principals que en formen part.

2.1.1 Criptografia

La criptografia es l'art y ciència de xifrar i desxifrar informació mitjançant tècniques especials i s'utilitza amb freqüència per permetre un intercanvi de missatges que solament poden ser llegits per les persones a qui van dirigits i posseeixen les medis per desxifrar-los. Dintre de la rama de la criptografia s'engloba com a tècnica complementària el *criptoanàlisis* que estudia els mètodes empleats per

trencat els texts xifrats amb intenció de recuperar la informació original amb absència de claus. Actualment es desenvolupen sistemes de seguretat que utilitzen la criptografia per assegurar la confidencialitat de les dades en qualsevol tipus de comunicació. En el entorn de la criptografia moderna es poden diferenciar dos clares vessants, la criptografia simètrica i la criptografia asimètrica o de clau pública. La primera es basa en algoritmes simètrics que utilitzen la mateixa clau per encriptar i desxifrar els missatges, contràriament la asimètrica es basa en algorismes de clau pública que utilitzen diferents claus per encriptar i desxifrar, on es mostra aquests dos tipus de criptografia (veure Figura 2.1)

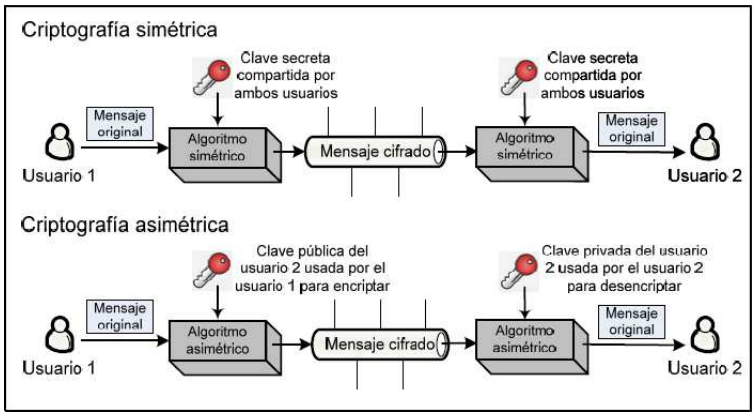

Figura 2.1: Mostra dels tipus de criptologia, Font:[url3]

2.1.2 El certificat digital i la signatura digital

En el procés de signatura digital, els algorismes de *hash* o "*hash codes*" tenen un paper important. Aquests algorismes són funcions de resum unidireccional i lliures de col·lisions. El valor obtingut després d'haver aplicat l'algorisme *hash* s'anomena valor del *hash* o simplement *hash* i té algunes característiques interessants com que el valor que es produeix en cada missatge és únic i és impossible la reconstrucció del missatge a partir del seu resum, per tant és un procés

no invertible que assegura la integritat de les dades. Els algorismes *hash* més coneguts actualment són el Message-Digest Algorithm 5 (MD5) i el Secure Hash Algorithm (SHA). En el procés d'obtenció de la signatura digital d'un missatge, l'involucrat posseeix dos pars de claus diferents que s'anomenen clau privada i clau pública. La clau privada és una clau pròpia que només coneix i posseeix el seu titular, essent-ne responsable de la seva custòdia per tal de garantir la fiabilitat del sistema. Aquesta clau està emmagatzemada en un dispositiu segur i s'ha de mantindre en secret, a diferència de la clau pública que pot ser coneguda per tothom sense cap mena de risc. La clau pública és necessària per comprovar la identitat de l'emissor, l'autenticitat del document i per desxifrar-lo, donat el cas. També s'ha acordar en un algorisme de signatura i en un algoritme de *hash* que s'utilitzaran tant pel signaturant com la persona que verifiqui la signatura. El primer pas és obtenir el valor *hash* del missatge i el segon pas el firmant ha d'utilitzar la clau privada per xifrar aquest valor *hash*, aquestes dues passes se les coneix com a signar digitalment un missatge i al resultat obtingut com signatura digital. La verificació de la signatura digital implica que una altra persona desxifri la signatura digital utilitzant la clau pública del firmant, si la pot desxifrar correctament pot confiar que el firmant realment va signar el missatge utilitzant la clau privada. El resultat de la verificació és el que es va encriptar amb la clau privada, en aquest cas el valor *hash* del missatge. En la figura (veure Figura 2.2) es mostra el procés d'obtenció de la signatura digital anteriorment esmentada.

La tecnologia de clau pública és fàcil i flexible, perquè permet que dues persones quan es troben s'intercanviïn les claus públiques i a partir d'aquí cada una d'elles pot verificar que els missatges que rep de l'altra són autèntics i íntegres. Si aquestes persones no es poden intercanviar les claus públiques personalment, esdevé la figura d'una tercera part de confiança que és la que s'encarrega de repartir les claus públiques. Per facilitar la distribució de les claus, aquesta entitat

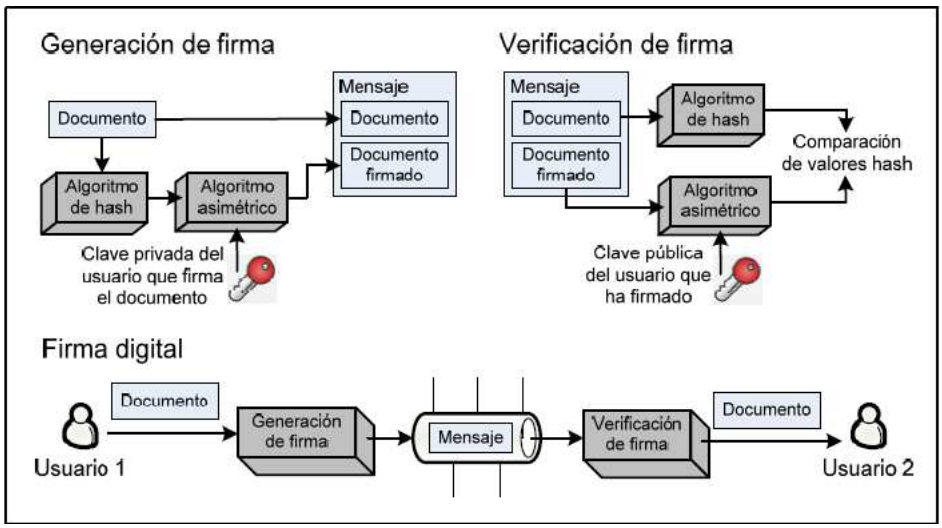

Figura 2.2: Procés de Firma Digital, Font [url3]

de confiança no dóna les claus públiques en mà, sinó que emet uns certificats que garantitzen que la clau que s'està distribuint pertany a una certa persona.

El certificat digital és un document electrònic format per un conjunt de requisits:

- Certificat digital = Dades del titular + Dades de l'entitat de certificació + Clau pública + Clau privada

L'Autoritat de Certificació (CA) és una entitat de confiança que s'encarrega de verificar les identitats certificades. El certificat digital permet al seu titular:

- Identificar-se davant tercers en establir comunicacions a través d'Internet.
- Assegurar que la seva identitat no és suplantada.
- Signar documents electrònics amb validesa legal.
- Protegir la confidencialitat de la informació tramesa.
- Garantir la integritat de la informació intercanviada entre dues parts.

I per tant, l'ús del certificat digital garanteix:

- La identificació de l'emissor. Només pot haver enviat la informació la persona que la signa.
- La integritat de la transacció. S'ha rebut tota la informació i aquesta no ha estat manipulada per cap persona no autoritzada.
- El no rebuig dels compromisos adquirits per via electrònica. La signatura electrònica reconeguda té el mateix valor legal que la signatura manuscrita.
- La confidencialitat de l'enviament. Una comunicació xifrada només pot ser llegida pel seu destinatari final i no pot haver estat manipulada.

En la figura (veure Figura 2.3) es mostra el procés de generació d'un certificat digital.

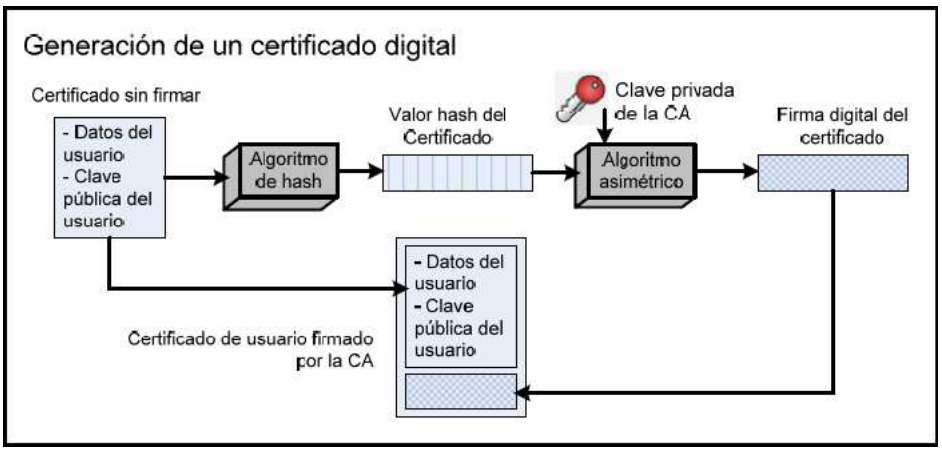

Figura 2.3: Generació d'un certificat digital, Font:[url3]

2.1.3 Infraestructures de Clau Pública

Una infraestructura de clau pública PKI es el conjunt de maquinari, programari ,persones, polítiques i procediments que ofereix el servei de crear, manipular,

emmagatzemar, distribuir i revocar certificats digitals basats en la criptografia asimètrica. Segons *William Stallings* (veure [Stallings]), el objectiu de construir una PKI es permetre l'adquisició de les claus públiques eficients, segures i convenients. El compliment d'aquesta premissa pot ser realment complicat i no degut a limitacions tecnològiques sinó perquè el problema resideix en la correcta implementació dels conceptes teòrics i la seva aplicació en els diferents entorns. Altrament s'observa en les empreses actualment grups de treball especialitzats en temes de PKI que es dediquen a desenvolupar i implementar el programari necessari per instaurar infraestructures de clau publica robustes i de confiança . Empreses com *IBM*, *Entrust*, *ChosenSecurity* ,*RSA Security*, *Cyber Trust*, *Safelayer* i *Microsoft*, entre d'altres, ofereixen solucions PKI en forma de productes gestionats pels prestadors de serveis de certificació.

2.1.4 Característiques de les PKI

Les infraestructures de clau pública tenen en compte quatre aspectes fonamentals, a continuació es comenta breument cada un d'ells i com la tecnologia PKI els estableix.

- **Confidencialitat**: Una comunicació entre dues persones no ha de ser vista ni interferida per una tercera persona que no en formi part. La tecnologia PKI utilitza el xifratge per assegurar la confidencialitat de les dades crítiques i sensibles que es troben en el canal de comunicació. També ofereix la possibilitat d'encriptar les dades sensibles emmagatzemades en els servidors que tenen connectivitat a Internet, això és important perquè en el cas hipotètic d'accés a les dades, es tindria que trencar el *criptosistema* per poder entendre el missatge. Cal ressaltar que el xifratge té un cost associat ja que les aplicacions desxifren les dades prèviament encriptades amb un alt cost computacional.

- **Autenticació**: Significa que es pot assegurar qui ha efectuat una certa activitat, ja sigui la generació d'un missagte o una acció sobre un recurs, fent ús de credencials d'identitat. La forma més comuna d'acreditar la identitat és a través d'un identificador d'usuari i contrasenya, aquesta forma esta considerada com a feble, amb un baix nivell d'autenticació i pot ser objectiu de ser trencada amb certa facilitat. La tecnologia PKI utilitza el certificat digital com a credencial d'identificació. Una companyia pot especificar en quines autoritats confia i això significa que solament accepta com a vàlids els certificats digitals emesos per aquestes autoritats. Un certificat digital pot ser guardat o en el navegador Web o en una Cryptographic Smart Card (CSC). La segona opció ofereix un grau mes elevat de seguretat ja que en el certificat digital mai es copia en disc. Normalment s'emmagatzema encriptat i protegit per un codi PIN/password en la targeta.

- **Integritat**: Les dades rebudes són les mateixes que les dades enviades, això vol dir que no són modificades o manipulades quan viatgen pel canal. Un altre aspecte que cuida la integritat és que es puguin provar innegablement que dos copies diferents del mateix missatge són idèntiques o no , tant en el present com en el futur. La tecnologia PKI utilitza els algoritmes textithash per assegurar la integritat de les dades. Aquests algorismes exploten la coherència d'un textithash, on el emissor amb un textithash preestablert informa al receptor del textit<hash del missatge, en el seu cas, el receptor compara el valor del textithash del missatge rebut amb el que va enviar el emissor, si els valors són idèntics es pot assegurar que el missatge no ha sigut modificat, el missatge manté la seva integritat.

- **No-Repudi**: Significa que si sorgeix una discrepància sobre el que ha succeït en una comunicació que implica el intercanvi de dades, hi haurà una

innegable evidencia present dintre del sistema de comunicació que pot ser utilitzada per provar amb la suficient certesa del que realment va succeir. Això es especialment sensible en operacions que impliquen la signatura de contractes electrònics per exemple, en les quals s'evitaria que qualsevol de les parts implicades en el contracte neguin lo abans signat. La tecnologia PKI proveeix del no repudiament a traves del ús de la signatura digital

2.1.5 Arquitectura de les PKIX

Com hem anat observant, els certificats digitals són una part fonamental de la tecnologia PKI. Els esforços per desenvolupar una arquitectura basada en certificats van consolidar el model d'arquitectura basat en certificats X.509 implementat per PKIX del Internet Engineering Task Force (IETF). Actualment el terme Infraestructures de Clau Pública X.509 (PKIX) es refereix a la infraestructura de clau pública basada en certificats X.509 i el terme certificat PKIX referent als perfils de certificació i llistes de revocació basades en l'estàndard X.509v3. El grup de treball PKIX han instaurat uns estàndards per satisfer els requeriments establerts per una PKI, específicament els Request For Comments (RFC) [RFC3280],[RFC2560] i el [RFC3161]. Els elements clau que composen el model arquitectònic PKIX són els següents:

- **End Entity (EE)**: Es el nom genèric que reben els usuaris d'una PKI o els dispositius que en formen part d' ella com encaminadors o servidors. Poden ser identificats en el camp del propietari del certificat X.509. Els usuaris fan ús normalment dels serveis oferts per la PKIX amb suport dels dispositius.

- **Certificate Authority (CA)**: Es l'autoritat encarregada d'emetre els certificats digitals X.509 i normalment també de les llistes de revocació de certificats (CRLs) , ocasionalment delega la funció d'emissió a un Emissor

de Certificate Revocation List (CRL). Tanmateix pot exercir funcions administratives com la de registre d'entitats finals o publicació de certificats però usualment aquestes funcions són realitzades per les autoritats de registre. Existeixen com a mínim dos tipus de CA en una jerarquia de certificació:

RootCA : CA arrel que emet els certificats a les CA de nivell inferior i el seu certificat ha sigut auto-signat.

SubCa: CA subordinada que emet els certificats a les entitats finals i on els certificats han sigut signats per l'autoritat de certificació arrel. En una poden existir varies CA subordinades a diferents nivells

- **Registration Authority (RA)**: Es un element opcional de l'arquitectura PKIX que pot assumir algunes funcions administratives de la CA, les mes comunes en el procés de registre de les entitats finals, tanmateix pot realitzar altres funcions com el procés de revocació de certificats i la manipulació de les dades de l'entitat . Dintre de la jerarquia de certificació poden existir vàries autoritats de registres de tipus intern o extern a la jerarquia de certificació del Prestador de Serveis de Certificació (PSC).

- **CRL issuer**: Es un element opcional de l'arquitectura PKIX on la CA pot delegar les funcions d'emissió de les CRL. Ocasionalment es troba integrat en la CA com a mode de servei.

- **Certificate Repository (CR)**: Aquest terme fa referència a qualsevol mètode existent per emmagatzemar certificats i CRL, per poder ser utilitzats posteriorment per les entitats finals. En certes jerarquies de certificació pot existir un sisè element que s'encarrega d'oferir informació sobre la vigència dels certificats digitals, es tracta en qüestió de la Validation Authority (VA) on es recull la informació quins certificats han sigut revocats anteriorment. Aquesta autoritat pot utilitzar el protocol Online Certificate Status Protocol

(OCSP) amb objectiu de prestació de serveis de validació ,donada que no esta inclosa en l'arquitectura PKIX perquè es usual que aquests serveis els presti la mateixa CA. En el cas hipotètic que es vulguin aïllar les dades de la comprovació de la vigència d'un certificat i credencials es recomana utilitzar una autoritat de validació diferent que la de certificació.

En l'arquitectura PKIX també es poden definir unes funcions de gestió, aquestes funcions s'expliquen a continuació:

- **Registre**: Procés on una entitat final registra les seves dades directament en una CA o per mitja d'una RA. També inclou procediments especials de mútua autenticació , on es generen clau privades compartides.

- **Inicialització**: Procés en que el client es registra de forma segura ,amb la seva clau pública i amb informació rellevant de la CA. La informació d'aquesta CA és la que utilitzarà per construïr el camí de validació dels certificats. Això és necessari perquè el sistema del client pugui operar satisfactòriament.

- **Certificació**: Procés on la CA crea un certificat que certifica que una determinada clau pública pertany a una entitat final i l'identifica de manera única i s'emmagatzema posteriorment en un repositori.

- **Recuperació par de claus**: Aquest procés permet a les entitats finals recuperar les seves respectives claus gràcies a una entitat prèviament autoritzada de recolzament de claus, normalment procedent de la mateixa CA que va emetre el certificat,la qual fa el rol d'aquesta autoritat. Aquesta funció es important perquè si s'ha perdut l'accés a la clau de desxifratge no es podrien recuperar les dades prèviament encriptades.

- **Actualització par de claus**: Procés pel qual en un temps determinat s'actualitzen les claus d'una entitat final i es torna a emetre el respectiu certificat. Normalment succeeix quan es compleix el temps de validesa d'un certificat o quan un certificat ha sigut revocat, per tant es tornen a generar el nou parell de claus.

- **Petició de revocació**: Es dóna quan una persona autoritzada dóna avís a la CA que ha succeït una anomalia o falla de seguretat i es demana la revocació del certificat d'una entitat final o usuari. Els motius de la petició poden ser en primer cas el compromís de la clau privada o en segon cas, un canvi de nom de l'entitat o fi del periode de vigència, entre altres.

- **Certificació encruada**: Procés on dues CAs intercanvien la informació necessària per emetre un certificat creuat. Aquest certificat és el que una CA arrel emet a una CA subordinada , sempre i quan aquesta última CA doni constància amb una clau de signatura autoritzada per emetre certificats,en la majoria dels casos d'entitat final.

A continuació es mostra en la figura (veure Figura 2.4) la interacció entre els elements del model PKIX anteriorment esmentats.

Aquestes funcions han de ser suportades per protocols de gestió de PKIX, actualment existeixen dos protocols definits en el grup de treball PKIX, un d'ells el protocol Certificate Management Protocol (CMP) definit en el [RFC2510] i que conté les funcions implementades. En una PKI existeix un document titulat " Practiques i polítiques de Certificació" , que tot PSC ha de tindre publicat per a la disposició del usuari. En altres coses, un PSC defineix les polítiques de certificació que s'esmenen per l'emissió de certificacions digitals.

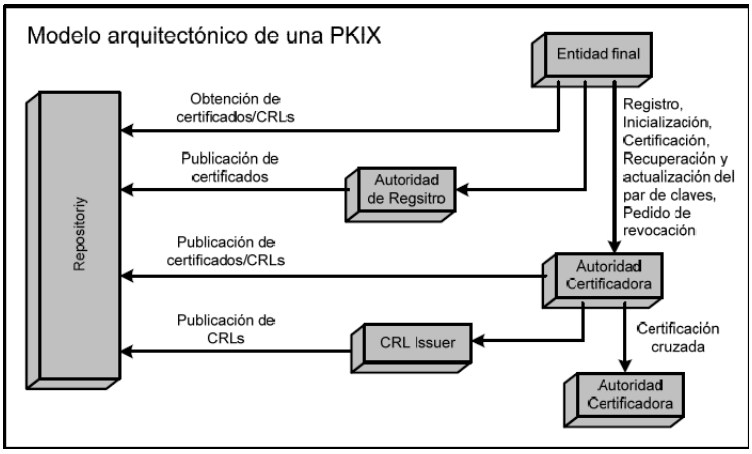

Figura 2.4: Model arquitectònic d'una PKIX, Font:[url1]

2.2 Models de confiança

Les PKI estan destinades a establir i mantenir relacions de confiança. Per tal d'assolir aquests objectius, els mecanismes per difondre la confiança dels organismes acreditats a entitats desconegudes han de ser implementats. Vegeu la secció 2.3 sobre els problemes vinculats a la interoperatibilitat en multi-domini de PKI. A continuació, s'examinen les propostes principals del model de confiança i els seus desafiaments més rellevants.

- **Model de CA Únic/Individual**: És la topologia d'arquitectura més senzilla,on existeix una única CA, on tots els certificats són emesos per una entitat emissora única. En el model únic de CA cada persona,el subscriptor disposa de la clau pública de CA en un lloc segur,fora de banda, i solament existeix un lloc per comprovar si un certificat ha sigut revocat. Aquest model sol ser ampliat pels RA, que estan allunyats de la CA, però són locals a grups d'usuaris específics. La RA es responsable de verificar la identitat del subscriptor i en cas necessari, les autoritzacions, abans d'aprovar la sol·licitud d'un certificat. Tanmateix, sovint fan la tasca d'establir una re-

lació de confiança preliminar entre el subscriptor i la CA, ja sigui a través d'un secret compartit, o mitjançant l'intercanvi de claus públiques.

Degut a la seva simplicitat, aquest model no és *escalable*, això condueix a l'aparició de múltiples entitats emissores de certificats interconnectades que gestionen comunitats d'usuaris inconnexes (veure Figura 2.5).

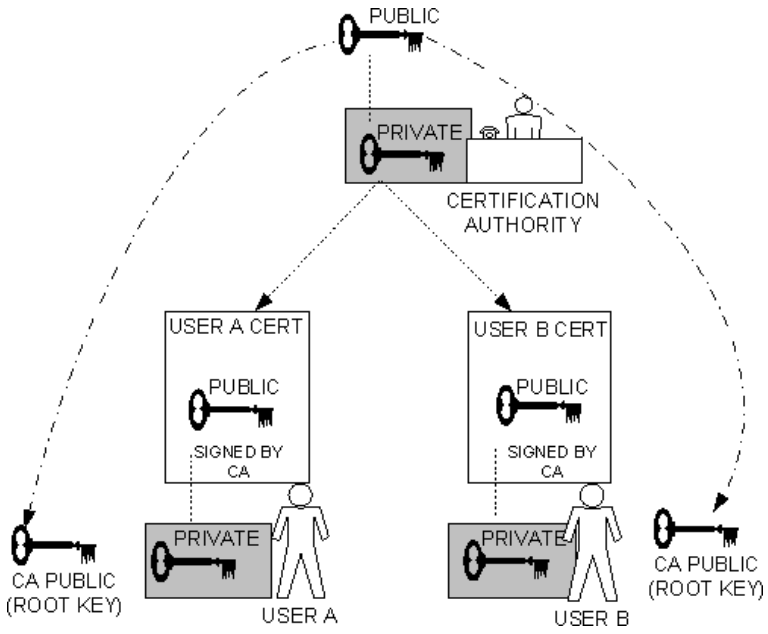

Figura 2.5: Model de CA únic, Font:[url1]

- **PKI jeràrquica** : El primer intent de resoldre el problema de la confiança en la interconnexió de múltiples illes era l'estructura jeràrquica de PKI que estava gestionada per una Root Certificate Authority (RCA). En aquest model , el camí de verificació de la cadena de confiança s'estableix en forma d'arbre amb el recorregut de dalt a baix *top-down*. La clau pública RCA és el punt fonamental de la confiança, per avaluar la validesa del certificat. No obstant això, la implementació d'una RCA única global és inadequada per raons polítiques (veure apartat introducció). No existeix un consens

sobre qui gestionaria la RCA i com ho faria (Jerarquia monopolista). Així doncs, la conclusió és que aquest model només és d'aplicació directa dins d'un domini administratiu, que es defineix com una zona establerta a certes polítiques i mètodes interns per forçar el compliment de les polítiques acordades (veure Figura 2.6).

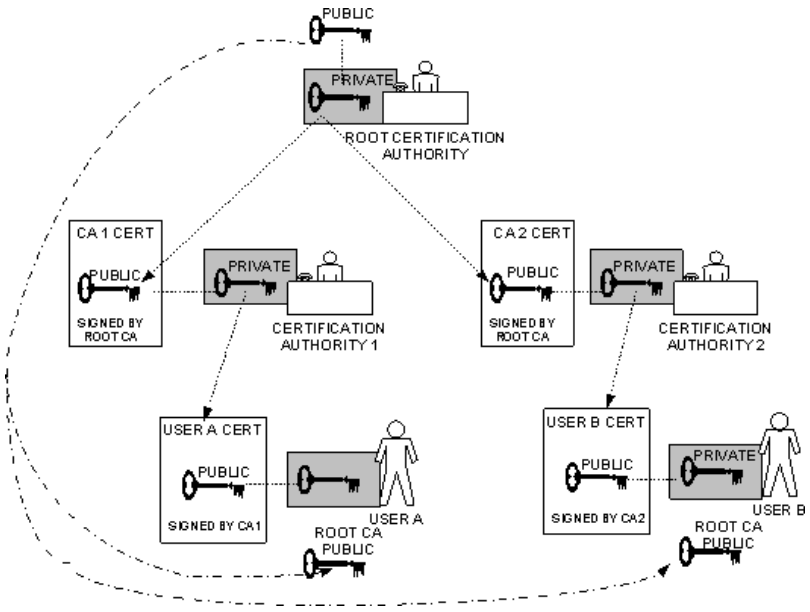

Figura 2.6: Model jeràrquic, Font:[url1]

- **Model de PKI en malla**: Hi han hagut múltiples esforços per aconseguir el desenvolupament de la confiança entre els nivells de domini. En el model de certificació encreuat, també conegut com a model de malla, dues CA que arriben al acord de confiar i dependre l'una de l'altra, expedeixen certificats de clau publica entre si, exactament es firmen recíprocament els certificats. El encreuament de certificats permet entre dues CAs, permet que els usuaris d'un domini administratiu puguin interaccionar electrònicament i de forma segura amb usuaris de l'altre domini. No obstant això, el nombre de certificats creuats tendeix a créixer de forma exponencial amb el nombre de

CA i les assignacions de la política són molt complexes. Per tant, apareixen problemes d'escalabilitat. D'altra banda, si un domini de PKI A vol unir-se a un altre domini de PKI B però limitant o impedint la confiança en un o més dominis que pugui tenir B afegits o s'hagi unit anteriorment,s'ha d'emetre un certificat d'encreuament amb B, amb una política restrictiva de forma expressa. Això fa que la construcció de camins de certificació entre dos CAs sigui encara més intractable. El Model de malla es pot basar en una arquitectura de PKI jeràrquica de manera que el nombre de certificats pot ser reduït per acotar la complexitat del sistema. Encara que IETF ha inclòs el model d'encreuament de certificats en la seu CMP i hi ha algunes implementacions de la mateixa,que encara no estan recolzades per a un ús de propòsit general en aplicacions com els navegadors o clients de correu electrònic. Això ens condueix a la necessitat de trobar un nou model amb complexitat lineal que interoperi amb diferents dominis de PKI (veure Figura 2.7).

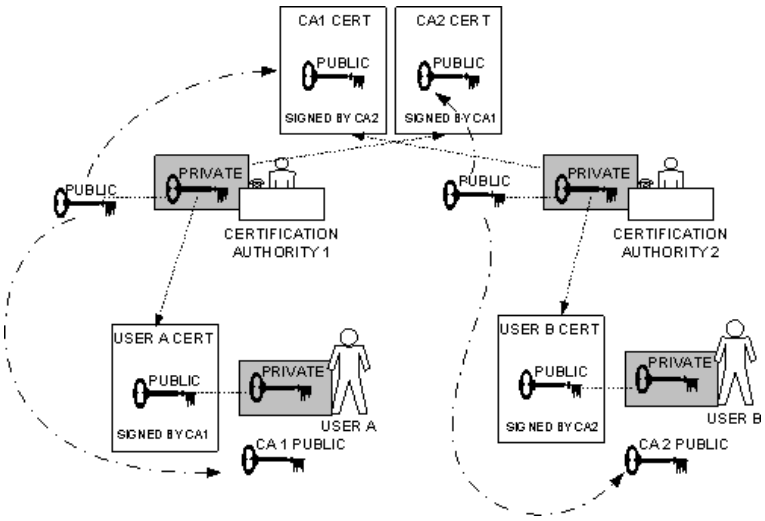

Figura 2.7: Model Mallat o d'encreuament de certificacions, Font:[url1]

En aquest projecte s'utilitza el terme llista de confiança per designar un

Figura 2.8: Model de llistes de confiança, Font:[url4]

conjunt de certificats signats de confiança, amb informació addicional, on es defineixen les propietats i les restriccions sobre la forma d'aplicar la confiança. Hi ha dos tipus de llistes de confiança:

Llistes de confiança dels usuaris : gestionat per un únic usuari.

Llistes del Proveïdor confiança : gestionat per un proveïdor de confiança.

El model de llista de confiança de l'usuari no presenta cap complexitat tècnica. No obstant això, s'ha de tenir en compte que els usuaris no tenen els mitjans o coneixements per construir la seva llista de confiança pròpia des de zero, perquè no saben ni les entitats emissores són capaços d'avaluar els riscos que comporta l'acceptació d'ells. Aquest és, per exemple, el cas de les sol·licituds del navegador web, que es distribueixen amb una llista predefinida de confiança units a ells per que els usuaris no han de crear-lo.

D'altra banda, les llistes de confiança de proveïdor són creats i administrats per un Trust Provider (TP). El seu objectiu és servir de referència per als usuaris, la confiança en els certificats de la llista és recomanat per un TP. Des de la perspectiva de la interoperabilitat de dominis, el proveïdor de la llista de confiança reemplaça essencialment l'encreuament de certificats entre CAs del model de malla. L'usuari confia en l'emissor de la llista, adopta la llista i llavors la confiança s'estén per cadascuna de les CA integrants de llista.

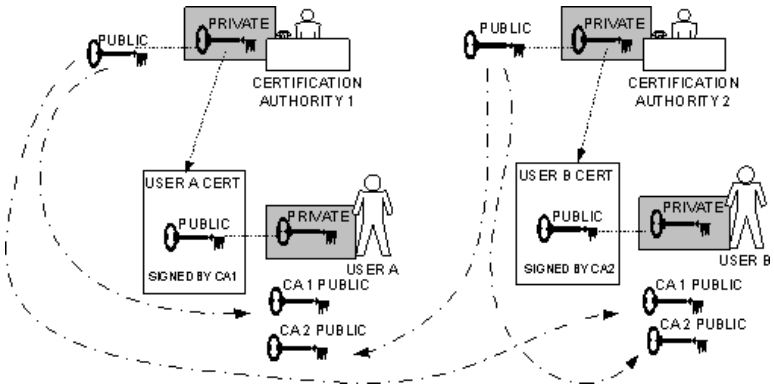

Figura 2.9: Model llista de confiança del navegador, Font:[url1]

- **Model pont entre CA** : Bridge Certification Authority (BCA) neix amb l'idea de facilitar la interconnexió de les diferents CA a través d'un procés encreuament de certificats. Cada usuari només confia en la seva pròpia CA que al seu torn confia amb el pont, el qual confia en una en una CA a distància,de manera que cada membre només ha de mantenir un híbrid simple de certificació amb la BCA i aleshores és capaç automàticament de construir rutes de certificació en totes les direccions. Cal assenyalar que el BCA no està destinada a ser utilitzada com una entitat de confiança per dels usuaris de la PKI. Simplement actua com una porta d'enllaç entre entitats emissores de certificats aïllades. Tot i així, BCA és responsable

d'assignar les polítiques de certificació i garantia d'equivalències de PKI adequadament. Per tant, els usuaris han de confiar-hi pel que fa a aquestes assignacions. Encara que aquest model és molt simple, des de la perspectiva de l'usuari final, de fet, presenta dificultats tècniques perquè la construcció de rutes de certificació són intrínsecament complexes i es requereixen de diverses comprovacions en tota la cadena de certificats. Cal destacar, a efectes pràctics que la certificació encreuada de CA es ser més tediosa i complexa respecte el model de llistes de confiança.

- **Model Pont de Validació entre CA**: Bridge Validation Authority (BVA) és un pas més respecte al BCA en el qual l'entitat central no és una CA, sinó una VA. Les VA són entitats externes *third parties* de confiança que els serveis en línia ofereixen en la validació de certificats. En termes generals, són responsables de la construcció de la ruta de certificació, l'avaluació de de la qualitat dels certificats, la validació del seu estat, i assegurar que estiguin vigents . En el model BVA, l'element que uneix a diverses illes de PKI és un VA que recull i classifica la informació d'estat de certificats de múltiples dominis. BVA es converteix en l'entitat de confiança per als usuaris i admet càrregues derivades dels certificats de que treballa. Aquest model resol algunes de les complexitats tècniques del BCA, per exemple,quan es tracta de construcció de rutes, ofereix als usuaris un servei més còmode. Tot i que simple, els usuaris estan totalment relegats a les decisions de la BVA i no reben cap informació sobre les característiques, la qualitat o context d'aplicació associats a la CA que estan treballant. D'altra banda, com ja hem vist en altres models, no pot existir una BVA única al món (Jerarquia monopolista), a causa de raons polítiques, sinó de diverses instàncies de les mateixes.

2.3 Multi-domini de PKI i la interoperabilitat

En un context de múltiples dominis de PKI, cada domini de PKI ha d'especificar les seves polítiques i les diferències entre la seva política i la dels altres dominis de PKI. Així, els casos d'ús què s'estableixen per la interoperatibitat en model de confiança han quedar reflectides en un Best Current Practices (BCP). Aspectes importants com els següents esmentats:

Relació de confiança : Aclariment de la relació de confiança en les PKI.

Dominis : Definició d'un domini de PKI.

Domini únic: La definició del model de domini únic de PKI.

Multi-Domini: La definició del model de multi-domini de PKI.

En la figura 2.10 es mostren el models de domini únic (Model únic de PKI i el Model jeràrquic de PKI i Model de PKI en malla) i multi-domini respectivament (Model per llistes de confiança i BCA)

Les relacions de confiança en les PKI es poden classificar en tres models, un model basat en llistes de confiança (veure Figura 2.9) , una certificació basada en el model de certificació encreuat (veure Figura 2.7) i model típic de jerarquia estricta (veure Figura 2.6).

La definició d'un domini de PKI és necessari per aclarir les fronteres en un context de múltiples dominis de PKI. Així doncs, per aclarir la diferència entre els dominis de PKI, hem de definir exactament quins elements intervenen. Per tant, modelar els casos d'ús típics en un model de confiança per un domini únic o multi-domini de PKI respectivament. A més d'això, la interoperabilitat per a la validació de ruta de certificació és necessària per verificar l'avaluació de les diferències de polítiques de confiança en aquests models.

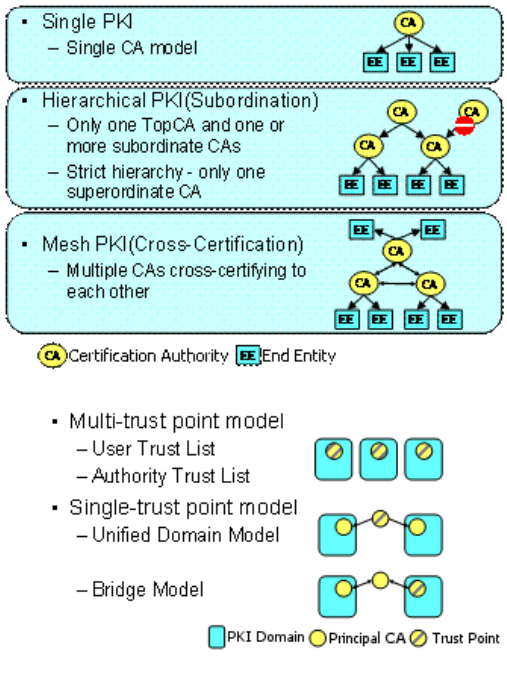

Figura 2.10: Models dels respectius dominis en les PKI, Font:[url2]

Alguns models com el BVA i les llistes de confiança tenen una gestió senzilla de la ruta de certificació,no obstant això, no ofereixen als usuaris detalls sobre paràmetres de qualitat de servei. Si una CA emet dos tipus de certificats amb diferents polítiques de seguretat,la part BVA estendrà el mateix tipus de respostes per als dos d'ells, sense incloure la informació de Quality of Service (QoS) referent a l'usuari. BCA ofereix un model de qualitat de servei a través de polítiques de certificació creuades. El BCA és responsable d'assignar la certificació i ha de publicar les normes de que segueix per acceptar la nova CA. No obstant això, aquesta arquitectura presenta complexitats tècniques que dificulten la interoperabilitat. Un altre repte dels models de confiança PKI és la forma d'ampliar la confiança i decidir si un certificat és de confiança per a un propòsit concret . Tot i algunes complexitats tècniques, el principal problema dels models de confiança existents és que no segueixen les directrius de confiança que utilitzem actualment en les relacions personals. Tanmateix,la creació d'una xarxa mundial de confiança uniforme no és viable. Els models proposats fins ara que admeten alguns personalitzacions són els basats en les llistes de confiança pero restringides a una mera classificació en diverses categories: certificats de confiança de les CA, els certificats web, els certificats de validació de codi i els certificats d'usuari final.

Diverses propostes han sorgit per formalitzar una política de certificació [NetCon], [RFC3647] i definir una forma d'interpretar les obligacions de les CA i la qualitat dels certificats que emet. A [EuroPKI2005] autors defineixen de forma automàtica per comparar els certificats de CAs i determinar la seva qualitat. L'ús de les regles estandarditzades de descripció faciliten l'avaluació del certificat. No obstant això, els usuaris no tenen els coneixements ni la capacitat per interpretar tots els paràmetres i prendre una decisió sobre la qualitat del certificat. Per tant, han de delegar aquesta operació a unes entitats externes, els TP que atorgaran confiança als usuaris i seran el referent del nou model proposat (Veure 4.1)

2.4 Comparativa de llistes de confiança

En la següent secció s'analitza en detall i es realitza una comparativa sobre el model de confiança basat en llistes, les seves particularitats i les variants en el model establert.

- **Model basat en llistes de confiança amb política**: La nostra llista de confiança ideal permetria restringir l'accés basant-se en la política en què es va expedir el certificat. Amb el desenvolupament d'un nou estàndard, com les llistes de certificats de confiança, sinó també considerant una política d'identificació mitjançant l'ús d'un Object IDentifier (OID) es podria integrar també, a les llistes de confiança d'altres entitats. Aquest model ens proporciona una gran precisió sobre quins certificats s'ha de confiar,això significa que una CA no s'ha de veure com una CA diferent per cada política de certificació que opera, cosa que redueix significativament els costos. No obstant això, actualment no hi ha suport del proveïdor per al filtratge de polítiques d'identificació per OID, tot i les recomanacions de fer-ho en el certificat Estandard ITU d'extensions de certificació (X.509v3) esmentades en el [RFC3280].

- **Model basat en llistes de confiança amb política i unitats organitzatives**: És com el model de la llista de confiança amb política, però en lloc d'utilitzar la política amb OID, volem establir un camp de certificat més ampli de suport, com a unitat organitzativa equivalent a un OID amb política. Aquest enfocament no ens dóna la capacitat d'integrar les llistes de confiança d'altres com l'anterior model, però no obstant és més flexible que el model per llista confiança del navegador. No obstant això, utilitzant les unitats organitzatives és encara una configuració personalitzada,el programari d'aplicació hauria de ser configurat per restringir l'accés, i algunes aplicacions de pro-

gramari que requereixen un desenvolupament personalitzat no treballarien correctament. La implementació requeriria una sèrie de configuracions, una respecte als responsables de triar a en quin certificat confiar per a l'autenticació (per a la llista d'entitats emissores de certificats), i la corresponent d'autoritzar l'accés a l'aplicació (unitat de filtratge). La llista de confiança basada en unitats organitzatives no és visible, i per tant es tornen complexes a mesura que afegim CA i polítiques gradualment, per tant, aquesta opció no és recomanable a causa de la dificultat en la configuració, i que no és basa en un enfocament estàndard.

La taula (2.11) resumeix els punts forts i febles de cada model. Podem observar la gran flexibilitat i diferenciació dels certificats per nivell de confiança en el model de llistes de confiança amb Unitat Organitzativa (OU), indicat per un entorn multi-domini de PKI, però tenim en contraposició que es un model no estàndard i amb difícil gestió de la configuració. No obstant, per solucionar aquesta problemàtica es proposa com a referent en el nou model de confiança basat en llistes de confiança la figura del Proveïdor de confiança (TP).

2.5 Ontologies

El concepte d'ontologia en informàtica proposa la creació d'un esquema dins d'un domini establert que té com a finalitat facilitar la comunicació i la compartició de la informació entre diferents sistemes. Les ontologies proporcionen els mitjans per a definir les relacions entre els objectes d'un domini. Aquesta informació és explotada en les llistes de la confiança com una manera de propagar automàticament la confiança en els certificats utilitzats en entorns similars. Per exemple, un TP pot recomanar un certificat perquè sigui acceptat en el context de serveis de no-repudiament en aplicacions d'aprenentatge. Per extensió, si un usuari se li

MODEL DE CONFIANÇA BASAT EN LLISTES	AVANTATGES	INCONVENIENTS
Model Únic	Barat i fàcil d'implementar Simple i ràpida des del punt de vista del usuari Total suport en aplicacions PKI	No existeix competència No existeix interoperativitat No es escalable
Model amb llista de certificats (navegador)	Fàcil d'implementar Molt flexible Total suport en aplicacions PKI Selecció de la AC de confiança	Potencialment més fàcils d'atacar L' usuari no gestiona la confiança
Model amb llista de certificats (política + OU)	Extremadament flexible Excel·lent diferenciació entre els tipus de certificat Potencialment menys cost de certificació.	Difícil de gestionar
Model Jeràrquic	La gestió es estructurada Potencialment robust Mínims problemes de interoperativitat	Qui posseeix la clau arrel (RCA) ? El enfocament de "top-down" no s'ajusta a la idea de una bona gestió Inflexible
Model Malla	No jeràrquic Raonablement flexible	La interoperativitat pot ser difícil Problemes amb la cerca una cadena de certificats
Model Pont	Pot vincular CA's de diferents dominis de PKI	La interoperativitat es molt complexa

Figura 2.11: Taula comparativa dels diferents models de confiança PKI

pregunta si s'accepta aquest certificat per els propòsits d'autenticació en un entorn *d'e-learning*, la resposta serà afirmativa. Ampliar el context de la utilització d'un certificat implica alguns riscos, per aquesta raó, el nivell de confiança d'aquest tipus de recomanacions sempre serà menor que els objectius marcats inicialment. L'aplicació del client serà la responsable de definir un llindar per sobre del qual els certificats seran acceptats o rebutjats.

Utilitzem ontologies per incloure totes les propietats i limitacions dels certificats emesos per les entitats emissores a la llista. La categorització dels certificats s'aconsegueix amb la informació de dos camps ortogonals (vegeu la figura 2.12):

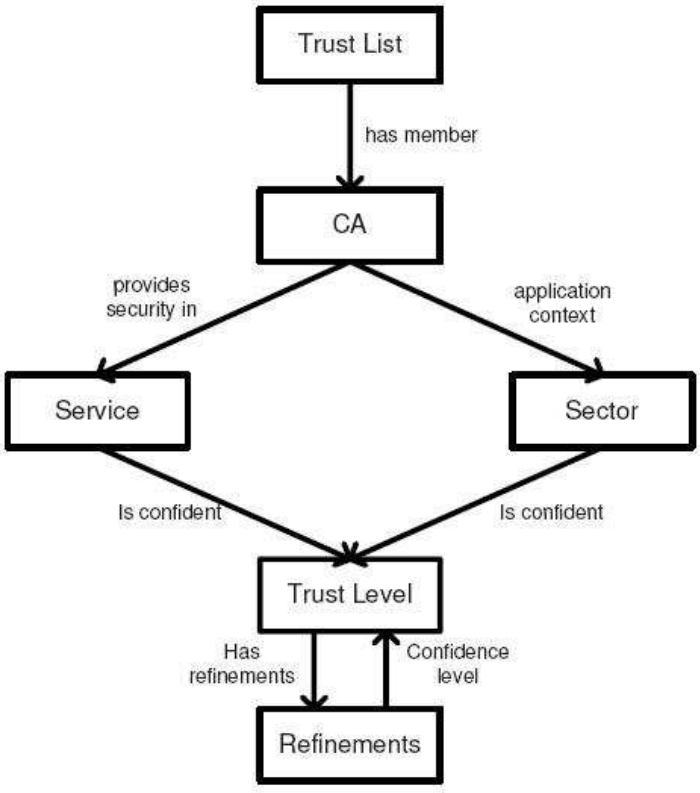

Figura 2.12: Ontologia en les llistes de confiança

Servei : Els serveis de seguretat que es concediran, com la identificació personal,

el control d'accés, el no repudi o l'establiment d'un canal segur.

Sector : L'àmbit de l'aplicació, és a dir, esports,banca, B2B, transport, oci, banca, etc..

El TP defineix un nivell confiança dels certificats, per un ús respectiu en cada sector (veure camps ortogonals) .

2.6 Resum

En aquest capítol s'han explicat el conjunt de conceptes previs necessaris per entendre el projecte. Així mateix s'han presentat tots els elements que conformen l'entorn on s'emmarca el projecte començant pels aspectes més generals com una introducció a les bases de la criptografia de clau pública i privada, la signatura i certificat digital i l'estudi dels respectius models de confiança. Finalment acabant amb conceptes més concrets com ara els estàndards i l'aprofundiment en detall sobre el model de llistes de confiança amb una comparativa final entre models i la definició d'una ontologia que estableixi les bases del disseny i funcionament del nou model.

Capítol 3

Anàlisi

En aquest capítol analitzarem els requisits que ha de tenir el model de confiança que es vol desenvolupar, així com també un breu estudi de viabilitat i alguns aspectes que caldrà tenir en compte en les fases de disseny i implementació. Finalment presentarem la planificació temporal prevista de les diferents etapes del projecte.

3.1 Anàlisi de Requisits

En aquest projecte es pretén desenvolupar el nou model de confiança basat en proveïdors de confiança. A continuació s'enumeraran els requisits que ha de tenir el model.

3.1.1 Requisits Funcionals

- Portable, per tant, independent de plataforma.
- El model ha de ser flexible, per tant ha de ser basat en una arquitectura modular.

- Orientat a connexió, per tant ha de treballar sobre TCP/IP.
- L'usuari ha de gestionar la confiança amb facilitat d'integració en el navegador.

3.1.2 Requisits No Funcionals

- El model haurà de respectar l'estàndard UIT-T X.509 per lesPKI.
- El model ha de suportar la versió 3 del X.509 que permet utilitzar camps opcionals.
- El model s'haurà de desenvolupar en el llenguatge de programació *Java*, donat la seva independència de plataforma.
- La integració en el navegador elegit, *Mozilla*, independent de plataforma, es farà mitjançant un *add-on* o *plugin* s'ha de implementar amb els llenguatge de programació Java Script (JS) i XML User Interface Language (XUL).

3.2 Estudi de Viabilitat

3.2.1 Viabilitat Tècnica

Aquest projecte es desenvoluparà amb el llenguatge de programació *Java*, juntament amb el llenguatges d'implementació de *plugins* JS, XUL. Serà necessari un treball previ de documentació i formació en relació a les eines i l'entorn de desenvolupament per cada mòdul,en aquest cas, s'ha utilitzat la plataforma de desenvolupament ECLISPE v3.2 per l'extensió de funcionalitat del certificat , que està previst en la planificació temporal del projecte. El projecte no requereix cap maquinari específic, simplement s'utilitzarà un ordinador estàndard amb el sistema operatiu GNU/Linux.

3.2.2 Viabilitat Econòmica

Tot el programari utilitzat per a la realització del projecte és programari lliure, per tant no suposarà cap cost afegit perquè no s'haurà de contemplar la compra de cap llicència. Com ja s'ha comentat a l'apartat de viabilitat tècnica, el sistema operatiu utilitzat és un Debian Lenny amb kernel 2.6.26-2-amd64 i l'entorn integrat de desenvolupament és l'Eclipse, editor Kate amb *highlighting* per diferents llenguatges. Per calcular el cost que suposaria desenvolupar el projecte, caldria aplicar el preu/hora de desenvolupament estipulat per cada empresa al nombre d'hores previstes per a la seva realització (descrit en l'apartat de Planificació Temporal del Projecte).

3.2.3 Viabilitat Legal

Tant la plataforma,com les llibreries de mozilla excepte les excepcions estipulades en la pàgina oficial,estan sota licència Mozilla Public License (MPL), GNU General Public License (GPL) i GNU Lesser General Public License (LGPL), així que no hi haurà cap restricció legal en quan al seu ús.

3.3 Planificació Temporal del Projecte

El projecte l'hem dividit en sis etapes. En l'etapa de documentació s'hi preveu l'estudi de l'entorn i les eines de desenvolupament que haurem d'utilitzar per a desenvolupar el projecte, així com l'estudi de l'estàndard X.509. Dins d'aquesta etapa de documentació també s'hi preveu la realització de l'informe previ del projecte que té com a data límit d'entrega el 17 de Abril de 2009. Un cop acabada la fase de formació específica per al projecte, ja es tindran els coneixements necessaris per a poder realitzar un anàlisi de requisits del nostre projecte que ens

permetrà fer un disseny adequat del model. Posteriorment s'iniciarà la fase d'implementació i proves, i preveiem un mes per a l'escriptura de la memòria. Val a dir que malgrat les etapes s'han disposat d'una manera seqüencial en la planificació, és de preveure que les fases de disseny i implementació i implementació i proves siguin etapes que segueixin un model evolutiu, fent ús del concepte de *backtracking* per poder resoldre els problemes que puguin anar sorgint al llarg del projecte.

Per a la realització del projecte s'estima una dedicació a temps parcial (mitja jornada) durant un semestre més una part prèvia de documentació i familiarització amb l'entorn i eines de desenvolupament. Amb tot es preveu una dedicació de:

28h Documentació + 26h Anàlisi + 21h Disseny + 118h Implementació + 20h Test + 64h Memòria = 277 hores.

3.4 Resum

En aquest capítol s'ha realitzat un anàlisi dels requisits que ha de tenir el nou model de confiança que es vol desenvolupar. A més a més s'ha fet un estudi de viabilitat del projecte on s'han analitzat i comentat aspectes tècnics, operatius, econòmics i legals del projecte a realitzar, així com també s'han introduït algunes idees que permetran començar a enfocar les fases de disseny i implementació del model. Finalment s'ha fet una planificació temporal del projecte on s'ha detallat una estimació del temps que es destinarà a realitzar les diferents fases del projecte.

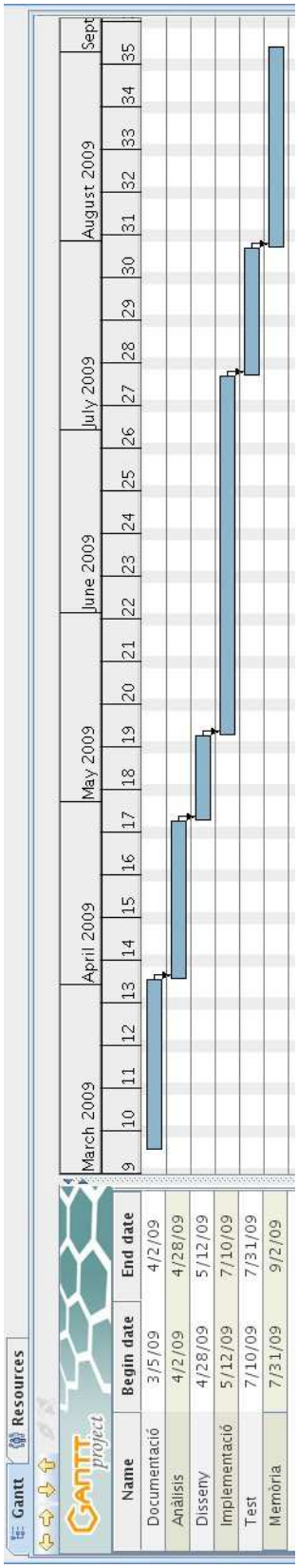

Figura 3.1: Diagrama de Gantt

Capítol 4

Disseny

En aquest capítol s'exposen les decisions de disseny que s'han pres per complir amb els requisits establerts en el capítol d'anàlisi. Així mateix, s'explica detalladament l'arquitectura, que permet estructurar la informació que s'intercanvien les diverses entitats.

4.1 Disseny del model segons requeriments

Un cop s'han concretat els requisits que ha de tenir el nou model de confiança basat en proveïdors de confiança i la definició de certs aspectes que haurà de complir el projecte, en la fase de disseny es veurà quines decisions s'han pres per garantir-los. A continuació es comentaran aspectes que s'han tingut en compte a l'hora de realitzar el disseny del nou model.

- El nou model ha de suportar l'ús d'un sistema de gestió de confiança on intervingui l'usuari final que estableix les seves necessitats o requeriments en cada moment, basat en la idea que s'ha anunciat en l'apartat 3.1.1, per tant, neix el referent del proveïdor de confiança.

4.2 Arquitectura del sistema

En aquesta secció es descriu l'arquitectura del nostre model de confiança destinat a facilitar l'interoperabilitat de multi-dominis de PKI. Les principals característiques de l'arquitectura proposada són:

- Construir un model de PKI centralitzat que estengui la confiança dels TP, entitats ben conegudes per part dels usuaris.
- Permetre als usuaris configurar la seva pròpia llista de confiança basades en les recomanacions del proveïdor de confiança, que poden ser acceptades o no.
- Facilitar la difusió de la llista de confiança i l'ús dels mecanismes bàsics de gestió de les PKI.

El nou model es basa en una arquitectura de diverses entitats que interoperen amb elements diferents,en la següent figura es detalla l'arquitectura del nou model de confiança basat en proveïdors de confiança (vegeu la Figura 4.1).

4.3 Entitats

Les entitats principals del nostre model són els usuaris, les autoritats de certificació (CA) i els proveïdors de confiança (TP). En la nostra arquitectura s'utilitza el terme usuari en un sentit ampli. Un usuari és una entitat que disposa de certificats i realitza les peticions de validació. Incís, aquest últim no ha de tenir un certificat obligatoriament,en alguns entorns, les entitats que validen els certificats es diuen les *relying parties* [RFC4158]. No obstant fem servir el terme usuari, en ambdós casos, per tal de simplificar la descripció.

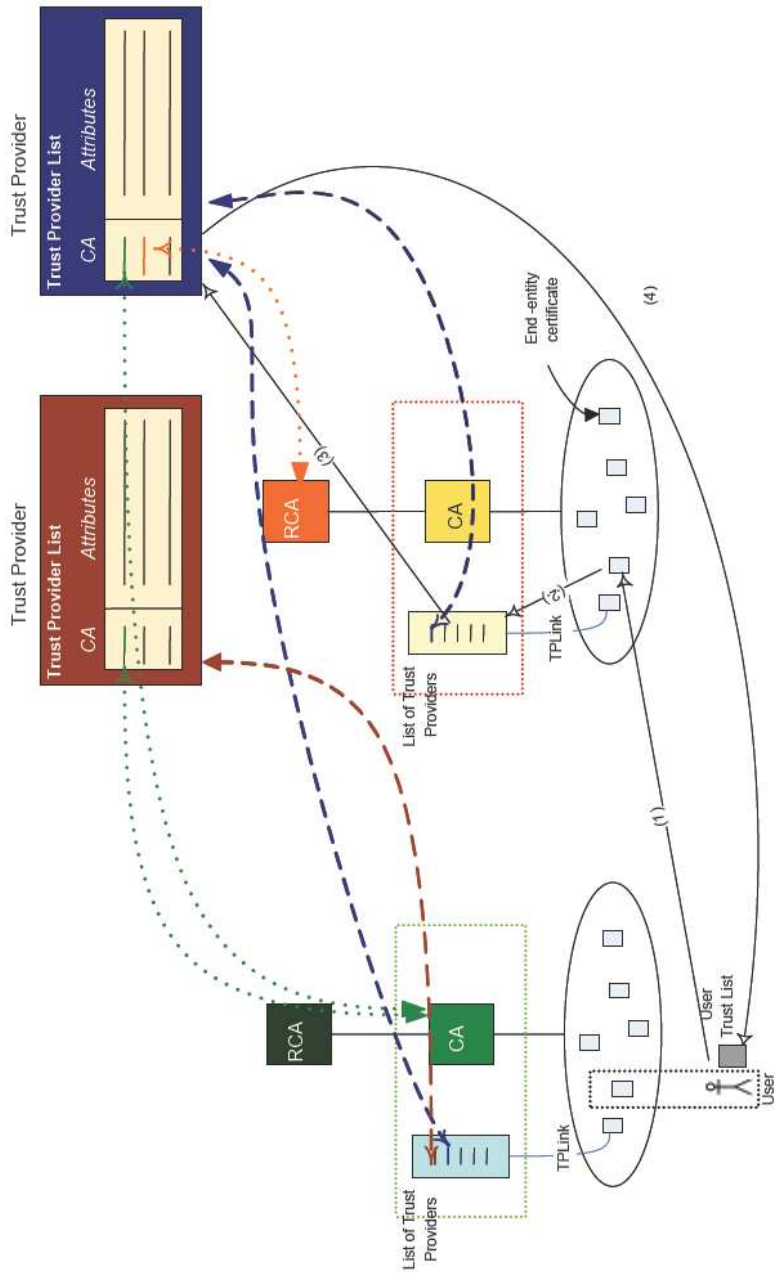

Figura 4.1: Arquitectura del nou model

- Autoritats de Certificació (CA). Són entitats que emeten certificats i donen fe de la unió entre els diferents elements de dades que trobem en els certificats. Les CA gestionen el cicle de vida dels certificats, la revocació si el certificat està compromés abans de finalitzar el període de validesa o la renovació de la validesa si ha de ser ampliada. Tanmateix, les CA han de mantindre sempre actualitzada l'informació dels certificats. L'Arrel de Certificació d'Autoritats (RCA) és un cas especial de CA en una jerarquia de nivell superior. És tracta de l'entitat de certificació on s'acabaran validant totes les cadenes de certificació que incorporin com a element final un certificat auto-signat, com a punt final de confiança de reconeguda validesa i reputació.

- Proveïdors de confiança (TP). Són entitats que són ben conegudes, que estan acreditades políticament, amb impacte jurídic o social (és a dir, el Ministeri de Justícia o el reconeixement de l'empresa privada). Gestionen les llistes de certificats de CA que es consideren fiables i que han assolit la qualitat necessària per ser utilitzades en alguns sectors especificats. El context d'aplicació dels certificats en la llista, es limita a l'àmbit d'influència del Proveïdor de confiança.

4.4 Elements principals

En la nostra arquitectura els elements principals són els certificats, la llista de proveïdors de confiança, les llistes de confiança, i una llista de motors d'execució de la confiança.

4.4.1 Certificats

Els certificats són el punt central de qualsevol model de PKI. La nostra arquitectura utilitza Certificats X.509 (veure [RFC3280]) en la qual implementarà una nova extensió de funcionalitat del certificat que anomenarem link o ellaç del proveïdor de confiança (TPL). Trust Provider Link (TPL) és una extensió de certificat no-crítica que conté ubicacions Uniform Resource Locator (URL), on s'indica l'ubicació de una llista de proveïdors de confiança es pot consultar. L'extensió del TPL és identificat per un identificador d'objecte (OID) únic:

Id	`id-pe-trustProvidersLink OBJECT IDENTIFIER ::= id-pe 20`
ASN.1	L'especificació en Abstract Syntax Notation One (ASN.1) de l'extensió es de la següent manera:
trustProvidersLink	`trustProvidersLink ::= SEQUENCE SIZE (1..MAX) OF TrusProviderLink`
trustProviderLink	`trustProviderLink ::= SEQUENCE accessMethod OBJECT IDENTIFIER, accessLocation GeneralName`

Taula 4.1: Estructura TrustProvidersLink (TPL)

En la taula 4.1,observem en detall, *trustProvidersLink* és una llista d'objectes *trustProviderLink* que contè la localització de les CAs publicades en la llista dels proveïdors de confiança.

4.4.2 Llista de TP

Una llista de proveïdors de confiança és una relació de diferents TP que soporten la política de unaCA. En la taula 4.2 es mostra els elements de la llista en llenguatge *XPath* [XPath]. Observar que les llistes dels proveïdors de confiança són signades prèviament per evitar manipulacions en les dades ,per tant, existeix un control de l'integritat. Es mostra en exemple especific en les figures 4.2 i 4.3.

```
- <List>
  - <TrustProvider>
      <Name>CN=TrustProvider, O=Ministry of Law, C=ES</Name>
      <Context>Law</Context>
      <Scope>Spain</Scope>
      <CertProvider>OU=FNMT Clase 2 CA, O=FNMT, C=ES</CertProvider>
      <Reference>https://www.minlaw.es/trust_provider/trust_list</Reference>
    </TrustProvider>
  - <TrustProvider>
      <Name>CN=TrustProvider, O=UOC, C=ES</Name>
      <Context>E-learning</Context>
      <Scope>Europe South-America</Scope>
      <CertProvider>O=UOC, C=ES</CertProvider>
      <Reference>https://www.uoc.edu/trust_provider/trust_list</Reference>
    </TrustProvider>
  - <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    - <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      - <ds:Reference URI="">
        - <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
          <ds:DigestValue>WScEsaC0y3PzG3cC9nUqLmTrnN8=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>gXqJmcIquM0PQjMWIziSXDiLHa6YhEmROorIMh65TEVdvA0c5bH1LJLVinC
        9od5nmarv8fIfF9Y/nDVW7Ad5NHcTYO+EOhyDA==</ds:SignatureValue>
    - <ds:KeyInfo>
      - <ds:X509Data>
          <ds:X509Certificate>MIIEIzCCAwugAwIBAgIBBDANBgkqhkiG9w0BAQUFADCBnjELMAkGAU
            G0+l2k2Y9fzfBqwx7OekTR+OQsMiTHuU/PvQq03uCcZHILF7Qw==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
  </List>
```

Figura 4.2: Llista de proveïdors de confiança

```
- <TrustList>
    <ThisUpdate>2007-03-02T09:16:16Z</ThisUpdate>
    <Target>Spanish citizens</Target>
    <Purpose>Social services access</Purpose>
    <From created="true" />
  - <Owner>
      <Id>CN=Medicus, C=ES</Id>
      <Name>Medicus, S.A.</Name>
      <Address>Calle Alcala, 43. 3-2 Madrid</Address>
      <URI>http://www.medicus.es</URI>
    - <Services>
        <Service>Health</Service>
        <Service>Insurances</Service>
      </Services>
      <BeginDate>1985-05-23T08:00:00Z</BeginDate>
      <Context>Public Health</Context>
    </Owner>
  - <CertList>
    - <CA rdf:ID="AC Raiz DNIE 01" xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
      - <CertProperties rdf:resource="#x509cert">
          <Subject>CN=AC Raiz DNIE, OU=DNIE, O=Direccion general de la policia, C=ES</Subject>
          <Issuer>CN=AC Raiz DNIE, OU=DNIE, O=Direccion general de la policia, C=ES</Issuer>
        - <Validity>
            <NotBefore>2006-02-27T11:54:38Z</NotBefore>
            <NotAfter>2021-02-26T23:59:59Z</NotAfter>
          </Validity>
          <EncodedCert>MIIFxTCCA62gAwIBAgIQZCBmyZl7ruFEAtpupCL9w0BAQUFADBdUE9MSU
            MQswCQYDVQQGEwJFUzEoMCYGA1UECgwfRElSRUNQUwgREUgTEEg</EncodedCert>
        </CertProperties>
      - <Constraints>
          <ProvidesSecurity rdf:resource="#NonRepudiation" />
          <ApplicationContext rdf:resource="#eHealth" />
          <TrustLevel>8</TrustLevel>
        </Constraints>
      </CA>
    </CertList>
  + <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  </TrustList>
```

Figura 4.3: Exemple de llista de confiança

XPath	Value
`/List`	Accés al contingut de la llista.
`/List/TrustProvider[n]`	Accés a l'informació al element enèssim del TP.
`/List/TrustProvider[n]/Name`	Nom del TP
`/List/TrustProvider[n]/Context`	Context d'operació del TP
`/List/TrustProvider[n]/Scope`	Àmbit d'influència del TP
`/List/TrustProvider[n]/CertProvider`	Certificat del TP ,si existeix.
`/List/TrustProvider[n]/Reference`	Localització de la llista de confiança URL
`/List/ds:Signature`	Signatura XML de la llista

Taula 4.2: Llista dels paràmetres del Proveïdor de confiança (TP)

4.4.3 Llistes de confiança

L'element principal de la nostra arquitectura són les llistes de confiança. Podem identificar dos tipus de llistes: Llistes de confiança dels usuaris i les llistes dels proveïdors de confiança, que són gestionades per TP, com nosaltres les coneixem com llistes de confiança dels proveïdors. Les llistes de confiança contenen tres grups d'informació:

- Dades del Propietari: Identifica l'entitat responsable de la llista de confiança. En el cas que aquesta entitat sigui la llista de TP és més fiable, per tant, inclou els serveis oferts pel TP, el nombre de clients que té, el propòsit de la llista i la seva finalitat. També s'indica si el TP és el refinament d'una llista de confiança existent, o creada des del principi.

- Llista de certificats: Llista de certificats de confiança i de classificació de la informació.

- Autenticitat de les dades: S'inclou els paràmetres per a validar la integritat i l'autenticitat de les dades que figuren en la llista. Aquests paràmetres inclouen un hash de les dades, la seva firma i el certificat de la signatura.

S'introdueix un format de llistes de confiança que permet definir els paràmetres de qualitat per als certificats. La taula 4.3 mostra els elements de la llista en el

XPath	Value
/TrustList	Accés al contingut de la llista de confiança.
/TrustList/ThisUpdate	Data de publicació.
/TrustList/Target	Objectiu
/TrustList/Purpose	Propòsit
/TrustList/From	Llista de TP
/TrustList/From/TrustProvider[n]	Informació el TP enèsim
/TrustList/From/TrustProvider[n]/Id	Nom complet
/TrustList/From/TrustProvider[n]/Update	Actualització
/TrustList/Owner	Informació del propietari de la llista
/TrustList/Owner/Id	Nom complet
/TrustList/Owner/Name	Nom persona jurídica responsable.
/TrustList/Owner/Address	Direcció
/TrustList/Owner/URI	Adreça web d'identificació única
/TrustList/Owner/Services	Llista de serveis associats
/TrustList/Owner/BeginDate	Creació a data específica
/TrustList/Owner/Context	Context operatiu
/TrustList/Owner/Market	Mercat del propietari
/TrustList/Owner/Status	Situació financiera del propietari
/TrustList/CertList	Llista certificats de confiança
/TrustList/CertList/CA[n]	Informació CA enèssima
/TrustList/CertList/CA[n]/CertProperties/	Ceritificat codificat i els camps
/TrustList/CertList/CA[n]/Constrains/	Restriccions
/TrustList/ds:Signature	Signatura XML de la llista

Taula 4.3: Paràmetres de les llistes de confiança (TL)

llenguatge XPath. El format de la llista es basa en l'especificació ETSI [ETSI] que s'ha estès per tal d'incloure els certificats de dades. Els TP avaluen els certificats que es volen incloure a la llista de confiança basada en el coneixement del titular de la CA i la qualitat dels certificats emesos (és a dir, el certificat de política de la CA).Els resultats de l'avaluació s'expressen en la llista utilitzant un llenguatge d'ontologies [Ontology].

4.4.4 Gestió a canvis de les llistes de confiança

Com que hi ha molts dominis independents i inconnexes de PKI en el món, les llistes de confiança dels usuaris han de ser actualitzades periòdicament per satisfer els canvis que es vagin produint . Els nous mètodes han de ser sempre la finalitat

de modificar i incloure la CA apropiada de la llista i els gestors de canvis en les llistes de confiança són l'eina adequada. Les llistes de confiança estan vinculades amb els gestors de la llista, que s'utilitzen per a codificar els requeriments dels usuaris i comprovar si els certificats compleixen les regles establertes d'acord amb la llista. El gestor és la interfície de les llistes de confiança que pot interpretar els requisits dels usuaris en llenguatge natural i automatitzar el procés de modificació i actualització de la llista propiament.

4.5 Estudi del cas d'ús i funcionament del model

4.5.1 Creació de llista de confiança del usuari

Les llistes de confiança dels usuaris són creades a partir d'importar la informació d'un proveïdor de la llista de confiança, d'una entitat que l'usuari coneix i confia. Per tant, els usuaris construeixen una llista de confiança pròpia basada en les recomanacions dels TP, que es van formalitzant en un TP referenciat en la llista de confiança. El TP pot oferir una interfície que permet la descàrrega i l'exportació només d'algunes parts de la llista (algunes emissores seleccionades). De tota manera, la informació que els usuaris accepten de les llistes dels proveïdors de confiança, pot ser refinada i després modificada pertinentment.

4.5.2 Gestió de la llista de confiança del usuari

Els proveïdors de confiança han de valorar i classificar els certificats en les llistes que es publiquen. Els usuaris poden perfeccionar o modificar aquesta classificació en les llistes gestionades per ells mateixos. Quan un usuari importa nou proveïdors de la llista de confiança a la seva pròpia llista, el gestor o motor de la llista de confiança, combina les dades amb el contingut dels altres proveïdors. En el nostre

model, l'ús de llistes de la confiança del usuari no és obligatòria. Hi ha una manera de fixar la validació de la confiança d'un certificat i garantir que el servei estarà disponible en qualsevol moment. No obstant això, els usuaris que necessiten verificar un certificat i no estan utilitzant el seus dispositius personals ni tenen accés a la seves llistes de confiança, poden realitzar la validació directament. Els motors o gestors de canvis de la llista de confiança dirigeixen l'usuari a una llista de TP, de la qual es fa referència en la validació del certificat, on l'usuari haurà d'indicar si confia en qualsevol dels TP de la llista i, si és positiu, la llista de confiança dels TP seleccionats serà consultada i les seves recomanacions importades.

4.5.3 Avaluació del certificat

En el model general, els usuaris mantenen una llista de confiança que conté els dominis dels TP en els quals hi confien. Quan estan involucrats en una transacció electrònica i és té la necessitat de decidir l'acceptació d'un certificat, es delega al gestor de la llista, la construcció de ruta de certificació i l'avaluació de si el certificat és prou fiable per al fi específic del certificat. Les entrades del gestor són el certificat en si mateix, i una descripció del context en que s'utilitzarà. Per exemple, observant el cas d'us (veure figura 4.4) un usuari pot demanar un certificat, si és admissible per al comerç electrònic. A fi d'avaluar el certificat pot ser demanat directament des de l'aplicació client, en aquest cas, el navegador web, on l'aplicació del client és la mateixa que passa les entrades contextuals al gestor de la llista de confiança.

La figura 4.1 mostra els passos de l'avaluació del certificat:

- Pas 1. El motor o gestor de la llista de confiança tracta de construir una ruta de certificació de confiança des del certificat d'usuari a una CA de confiança de la llista. Si és incapaç de fer-ho, pot ser perquè no coneix l'autoritat, o perquè la coneix pero l'usuari no confia explícitament en ella. En el primer

cas, com el certificat avaluat té una extensió de TPL, a través de la qual el gestor pot obtenir més informació sobre ella, exactament sobre quin és el domini de PKI al qual pertany, a través de les recomanacions realitzades per alguns TP. Els punts d'extensió TPL per una llista de TP poden subministrar més informació sobre la cadena de certificació no coneguda previament.

- Pas 2. El gestor de l'aplicació es connecta a la pàgina web en la qual la CA que ha emés el certificat publica una llista de TP. Tots els TP estan la llista de suport de la CA, però, el context i l'abast de cada proveïdor és diferent. Si la llista del TP no està disponible, el certificat avaluat es considera no confiable i s'acaba el procés d'avaluació. En cas contrari, després de rebre la llista de TP on s'ha verificat que és autèntica, el gestor cerca si l'usuari coneix alguns dels proveïdors, és a dir, comprova si els TP estan registrats a la llista de confiança dels usuaris. Si és el cas, s'accepta la recomanació dels TP registrats. En cas contrari, el gestor li pregunta al usuari si vol importar alguns TP nous en el dipòsit i actua en conseqüència.

- Pas 3. Els TP són acceptats. El client verifica la signatura de les llistes de confiança dels TP.

- Pas 4. Les llistes de confiança dels TP es descarreguen i es fusionen amb la informació actual de la llista de confiança dels usuaris. Quan les recomanacions d'un domini de PKI vénen de diversos proveïdors de confiança, el que té millor nivell de confiança són el valor que prevaleix. Si la informació dels proveïdors de confiança ha de ser combinada amb les dades indicades per l'usuari, propietari de la llista, el dictamen del usuari té preferència , donat els requeriments del model que estableixen l'usuari com a element únic de decisió de la confiança (veure 3.1.1).

En un cas d'ús, exemplificat en la figura 4.4 podem establir les següents pas-

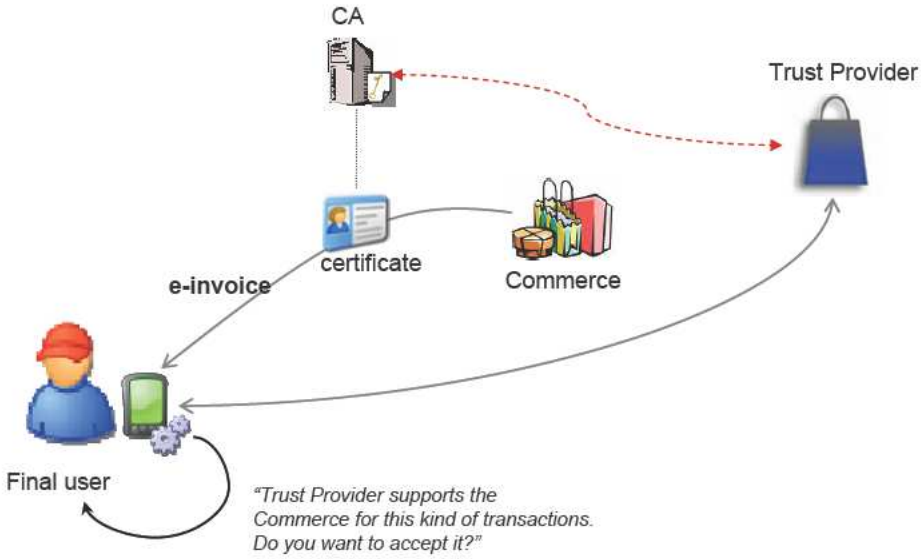

Figura 4.4: Cas d'ús del model de confiança basat en TP

ses:

- Pas 1: En Carles navega per Internet i es connecta a una pàgina de *e-commerce* per la compra de uns productes.
- Pas 2: No obstant això, el venedor li presenta un certificat de que no reconeix ,ja que no es troba en la llista de confiança del usuari.
- Pas 3: Li demana al gestor o motor de la llista de confiança verificar la validesa de del certificat per serveis de comerç electrònic.
- Pas 4: El gestor comprova que el certificat del proveïdor és emès per una CA que és membre de les llistes de certificats de confiança dels principals proveïdors de programari i que el context d'aquesta CA és el comerç electrònic. Es demana a en Carles, si confia en el TP de la llista, com que la resposta és afirmativa, el gestor valida el certificat del proveïdor de confiança i en Carles és capaç de realitzar la compra amb garantia de confiança.

4.6 Resum

En aquest capítol s'ha explicat el disseny del nou model de confiança basat en proveïdors de confiança que s'ha fet atenent als requisits establerts en el capítol d'anàlisi. S'ha explicat amb detall les entitats integrants del model, els elements principals, les defincions i exemples de les llistes de confiança de les entitats en cada cas. Finalment s'ha mostrat un cas d'us del nou model, on es defineix el funcionament i es planteja un cas pràctic.

Capítol 5

Implementació

En aquest capítol s'explica com s'ha organitzat el codi a partir del disseny del model, així com les decisions d'implementació que s'han pres a raó dels requeriments (veure 3.1) del model. Finalment es presentaran porcions de codi per exemplificar cadascun dels mòduls.

5.1 Mòduls del model de confiança

En la següent figura 5.1 podem observar diferents cercles de colors, groc, vermell, blau i gris respectivament que especifiquen els diversos mòduls que s'implementaran. Podem aleshores agrupar i establir 3 mòduls ben diferenciats:

- (GROC) Mòdul *add-on o plugin* en el navegador: Interfície per la qual l'usuari podrà gestionar la confiança, consultar, acceptar o declinar les recomanacions del proveïdor de confiança.

- (VERMELL) Mòdul d'extensió de funcionalitat, el TPL X.509v3: Permetrà al usuari consultar l'ubicació de la llista de confiança del proveïdor segons el context d'aplicació que es tracti.

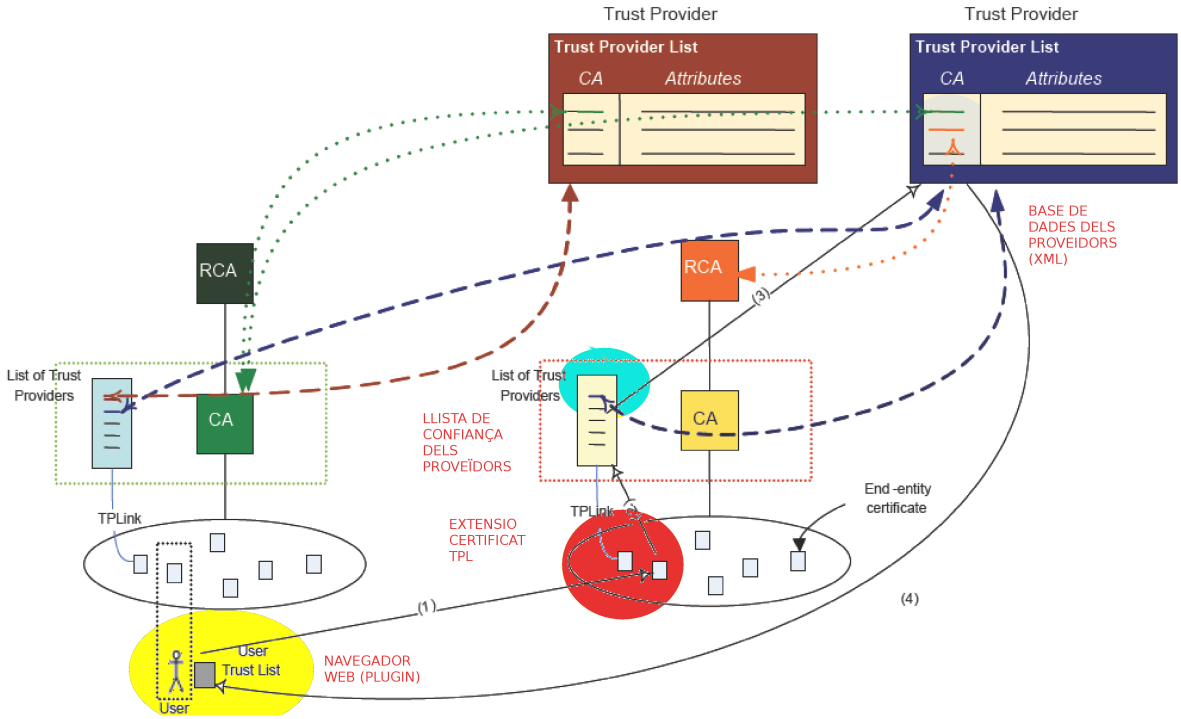

Figura 5.1: Mòduls del model de confiança

- (BLAU i GRIS) Mòdul de la llista de confiança amb la base de dades dels proveïdors de confiança: Ubicació on resideixen les llistes de CAs del proveïdors de confiança classificades segons els atributs en un context d'aplicació, estructurat en *tags* Extensible Markup Language (XML).

5.1.1 Mòdul del Navegador WEB

Segons els requeriments del nou model (veure 3.1) s'estableix la premissa funcional del model en un entorn multi-plataforma. Justament dintre d'aquest context d'aplicació , s'emmarca l'extensió i gestió dels certificats en forma d'una extensió integrada dintre de l'entorn *Mozilla*. Dintre d'aquest l'entorn tractarem amb les següents tecnologies :

- XUL: Llenguatge basat en XML per la interfície d'usuari. És una aplicació

de XML feta per *Mozilla*, i es fa servir en els seus projectes i en d'altres. XUL només proporciona la part gràfica, per tant, s'ha de fer servir amb altres llenguatges de programació per implementar la lògica de control, en el cas del JavaScript.

- JS: JavaScript és un llenguatge script basat en el concepte de prototip, implementat originàriament per *Netscape Communications Corporation*, i que va derivar en l'estàndard [ECMAScript]. És conegut sobretot pel seu ús en pàgines web, però també s'utilitza en altres aplicacions per oferir fluxos de control.

- Cross Platform Component Object Model (XPCOM): Model de components de la plataforma de Mozilla. Té descripcions Interface Definition Language (IDL) perquè els programadors puguin gestionar els components, tal com ,fer abstracció del contingut, pas de missatges entre objectes i gestió de la memòria. En aquest projecte, finalment no ha estat necessari la generació funcional d'un component XPCOM donat que amb JS es proveeix de tota la funcionalitat requerida per l'extensió. Tanmateix, s'ha generat un esquelet per una possible ampliació del plugin sota un marc de web semàntica.

En la Figura 5.2 es mostra la implementació gràfica del *plugin* amb XUL i posteriorment el JS ofereix la lògica de control necessària mitjançant la crida de funcions dintre de XUL.

El navegador web juntament amb la integració de l'extensió *"TrustProvider"*, permetrà a l'usuari gestionar l'elecció de la confiança segons un context d'aplicació. Tanmateix, podrà accedir a la llista de confiança que n'és propietari i consultar als proveïdors de confiança pertinents per anar acceptant o declinant les recomanacions que es vagin generant.

```
<?xml version="1.0"?>
<?xml-stylesheet href="chrome://TrustProvider/skin/TrustProvider.css"
                 type="text/css"?>

<overlay id="trustprovider" xmlns="http://www.mozilla.org/keymaster/gatekeeper/there.is.only.xul">

  <!-- scripts start -->
  <script type="application/x-javascript" src="chrome://trustprovider/content/TrustProvider.js"/>
  <!-- scripts end -->

  <statusbar id="status-bar"> <!-- overlay firefox statusbar -->
      <statusbarpanel id="hf_Status"
                      context="hf_StatusContextMenu" >

      <image id="hf_StatusLogoImage" tooltiptext="TrustProvider" />
      </statusbarpanel>

  <menupopup id="hf_StatusContextMenu" onpopupshowing="">
        <menuitem
        label="Finestra Certificats"
        oncommand="toOpenWindowByType('mozilla:trustprovider',
        'chrome://pippki/content/certManager.xul');"
        image="chrome://trustprovider/skin/application_double.png"/>
        <menuitem
        label= "Informacio Projecte"
        oncommand="TrustProvider.doOpenTool_newTab('chrome://trustprovider/content/info/projecte.html');" />

        <menuseparator/>

        <menuitem
          label="Options"
          oncommand="TrustProvider.OpenOptions();"/>
          <menuitem
          label= "Filtratge DB"
          oncommand="TrustProvider.FilterDB();" />

      </menupopup>
```

Figura 5.2: Codi XUL amb instanciació de funcions JavaScript

5.1.2 Mòdul d'extensió de funcionalitat del certificat X.509v3

Es tracta de la generació de un TPL, una extensió de certificat no crític que permet al usuari saber on estàn ubicades les llistes de confiança per un context d'aplicació concret. Segons els requeriments (veure 3.1), l'extensió del certificat es farà amb *Java*, dintre d'aquest context, tenim vàries opcions per la implementació del TPL amb les Application Programming Interface (API) corresponents.

- Llibreries *Bouncy Castle*: Es un projecte software lliure que pretén desenvolupar una sèrie de llibreries criptogràfiques lliures, en altres, ofereix un *provider* pel Java Cryptography Extension (JCE) de *Java*

- Java Security Services (JSS): JSS es una interfície *Java* desenvolupada per *Mozilla* per a la seva llibreria Network Security Services (NSS), donant suport quasi a tots els estàndards de seguretat i xifrat definits en la NSS. També proporciona una interfície per a tipus ASN.1 i codificació Basic Encoding Rules (BER)/DER.

- *IAIK*: El proveïdor de *IAIK* de (IAIK JCE) és un conjunt d'APIs i implementacions de funcionalitats criptogràfiques, incloent les funcions hash, codis d'autenticació de missatges, simètrica, asimètrica, el xifrat de bloc, clau i gestió dels certificats. Així mateix, complementa la funcionalitat de seguretat del Java Development Kit (JDK).

L'elecció de la implementació de l'extensió de funcionalitat del certificat, basant-nos en les especificacions X.509v3 es amb l'ús de les llibreries **IAIK**. Les justificacions són les següents:

- El major problema del JSS és la seva gran dependència de configuració amb l'aplicació del client.

- La pròpia JSS ,en si mateixa, no sembla tindre clar el camí a seguir per ajustar-se a les especificacions de l'arquitectura Java Cryptography Architecture (JCA), sense la implementació de una clase *KeyStore* estàndard i amb un format tancat per els repositoris de claus.

- El NSS permeten un accés total a les funcions de la llibreria interna NSS, sense tenir que utilitzar envoltoris per altres llenguatges, com és el cas de JSS. Tenim la contrapartida, que té una documentació escassa i no es té constància de la possibilitat de creació d'extensions de certificats X.509v3

- En el cas, *IAIK* ens proveeix d'informació detallada i concisa del *provider* i ens ofereix mètodes que permeten l'extensió de certificats X.509v3.(veure figura 5.3 i documentació [JCE-IAIK]).

Classes implementades i dependències de les llibreries IAIK

S'han creat i implementat les classes seguents segons els requeriments establerts (veure 4.1)

- CertificateExtensions.class: Classe principal on es defineixen tots els camps que es llisten a continuació i es genera el certificat. (veure Figura 5.3)

  AuthorityKeyIdentifier: Identifica la clau pública de la CA amb la que es va firmar el certificat.

  BasicConstraints: Especifica si el subjecte del certificat és una CA i la profunditat de la ruta de certificació que pot existir a través d'aquesta CA.

  PolicyQualifierInfo: La política en les que el certificat ha estat emès i els fins per als que el certificat podrà ser utilitzat.

  CRL distribution point: La Uniform Resource Identifier (URI) o localització de la llista de certificats revocats.

IssuerAltName: Emissora d'extensió del nom d'alternatives per a associar les identitats estil d'Internet amb l'emissor del certificat

KeyUsage: Usos que se li poden donar al parell de claus, camps d'aplicació.

NameConstraints: Indica un espai de noms, en el qual tots els noms d'objecte dels certificats posteriors en una ruta de certificació han d'estar ubicats.

PolicyConstraints: Especifica l'extensió de la política d'assignacions que s'utilitzaran en els certificats de CA per a la inclusió d'un o més parells d'identificadors d'objectes, cadascun d'ells inclou un issuerDomainPolicy i subjectDomainPolicy

PolicyMappings: Pot ser utilitzat per prohibir l'assignació de polítiques o exigir que cada certificat en una ruta d'accés conté un identificador de política acceptable.

PrivateKeyUsagePeriod: Especificar un període de validesa diferent de la clau privada del certificat.

SubjectAltName: Permet vincular altres identitats addicionals del certificat

SubjectKeyIdentifier: Identifica la clau pública de l'entitat certificada.

AuthorityInfoAccess: Descriu el format i la ubicació de la informació addicional sobre la CA que va emetre el certificat en el qual apareix aquesta extensió.

TrustProvidersLink: La URI o localització de les entitats de confiança del TP. Aquestes CA formaran part de la llista de l'usuari on s'estendrà la confiança gràcies a les recomancions del proveïdor.

- TrustProviderLink.class: Classe que implementa una seqüència formada per dos mètodes, exactament un *accesMethod* on s'estableix un OID, que ens servirà per identificar la manera única l'objecte i un *AccessLocation* GeneralName per indicar-li un nom.

- TrustProvidersLink.class: Classe que implementa l'extensió de funcionalitat del certificat X509v3, amb OID únic , estructura definida com una seqüència de 1-n TrustProviderLink. Englobat en *V3Extensions* juntament amb les altres extensions del certificat.

A continuació es mostra en detall la implementació les classes *TrustProviderLink i TrustProvidersLink* anteriorment citades, en aquesta última s'expliquen els mètodes sense detallar el codi per evitar una sobredimensió del projecte. Tanmateix si es vol aprofundir més en les implementacions es podran consultar des del material adjunt (Compact Disc (CD)), on hi haurà contingut tot el material del projecte.

```
public class TrustProvidersLink extends InfoAccess
{
 public int hashCode()
 {
     return oid.hashCode();
 }
 public ObjectID getObjectID()
 {
     return oid;
 }
 public TrustProvidersLink(TrustProviderLink accessdescription)
     throws IllegalArgumentException
 {
     super(accessdescription);
 }
 public TrustProvidersLink()
 {
 }
    public static final ObjectID oid = new ObjectID("1.3.6.1.5.5.7.1.11", "TrustProvidersLink");
```

```
}

public class TrustProviderLink
    implements ASN1Type
{

    public String toString()
    {
        ...
    }

    public ASN1Object toASN1Object()
        throws CodingException
    {
       ...
    }

    public void setUriAccessLocation(String s)
        throws IllegalArgumentException
    {
       ...
    }

    public void setAccessMethod(ObjectID objectid)
        throws IllegalArgumentException
    {
       ...
    }

    public void setAccessLocation(GeneralName generalname)
        throws IllegalArgumentException
    {
       ...
    }

    public String getUriAccessLocation()
    {
        ...
    }

    public ObjectID getAccessMethod()
    {
```

```
        return a;
    }

    public GeneralName getAccessLocation()
    {
        return b;
    }

    public void decode(ASN1Object asn1object)
        throws CodingException
    {
        ...
    }

    public TrustProviderLink(ObjectID objectid, String s)
        throws IllegalArgumentException
    {
        ...
    }

    public TrustProviderLink(ObjectID objectid, GeneralName generalname)
        throws IllegalArgumentException
    {
       ...
    }

    public TrustProviderLink(ASN1Object asn1object)
        throws CodingException
    {
        decode(asn1object);
    }

    public TrustProviderLink()
    {
    }
    private GeneralName b;
    private ObjectID a;
}
```

Addicionalment s'han realitzat modificacions adients en les classes següents, per resoldre dependències:

- InfoAccess.class on s'ha afegit el domini i l'estructura TrustProviderLink.
- X509Extension.class on s'ha afegit el domini i l'estructura TrustProvidersLink.
- V3Extension.class s'ha realitzat el canvi del tipus de dades a TrustProvidersLink en els paràmetres d'entrada de certs mètodes

En les següents imatges es pot veure la extensió del certificat vista amb les llibreries NSS des del navegador (veure Figura 5.4) i la visualització del certificat amb *OpenSSL* (veure figura 5.5) amb la comanda:

- **openssl x509 -in ./ecommerce.crt -text -noout**

```
    ////TrustProvidersLink//////
    ObjectID accessMethod_TP = new ObjectID("1.3.6.9.9.9.9999.9.9.9.9.9.9", "TPL");;
    GeneralName accessLocation_TP = new GeneralName(GeneralName.uniformResourceIdentifier, "https://www.e-commerce.es/trust_provider/trust");

     TrustProviderLink trustProviderLink = new TrustProviderLink(accessMethod_TP, accessLocation_TP);
     TrustProvidersLink trustProvidersLink = new TrustProvidersLink(trustProviderLink);
     extensions.addElement(trustProvidersLink);


    V3Extension[] e = new V3Extension[extensions.size()];
    extensions.copyInto(e);

    X509Certificate cert = createCertificate(subject, privateKey.getPublicKey(), subject, privateKey,
          AlgorithmID.sha1WithRSAEncryption, null, 12345, e);

    byte[] test = cert.toByteArray();
    // send certificate to ...
    iaik.utils.Util.saveToFile(test,"/home/counter/workspace/ecommerce2.crt");


    // receive certificte
    X509Certificate new_cert = new X509Certificate(test);
    System.out.println(new_cert.toString(true));

  } catch (Exception ex) {
    ex.printStackTrace();
    throw new RuntimeException();
  }
}
```

Figura 5.3: Codi Java amb les llibreries IAIK per generar l'extensió de funcionalitat TPL

5.1.3 Mòdul de la llista dels proveïdors de confiança

En aquest cas, la llista de proveïdors de confiança s'estructuren en XML, amb el corresponents *tags* que permeten detallar cada camp i realitzar una estructura

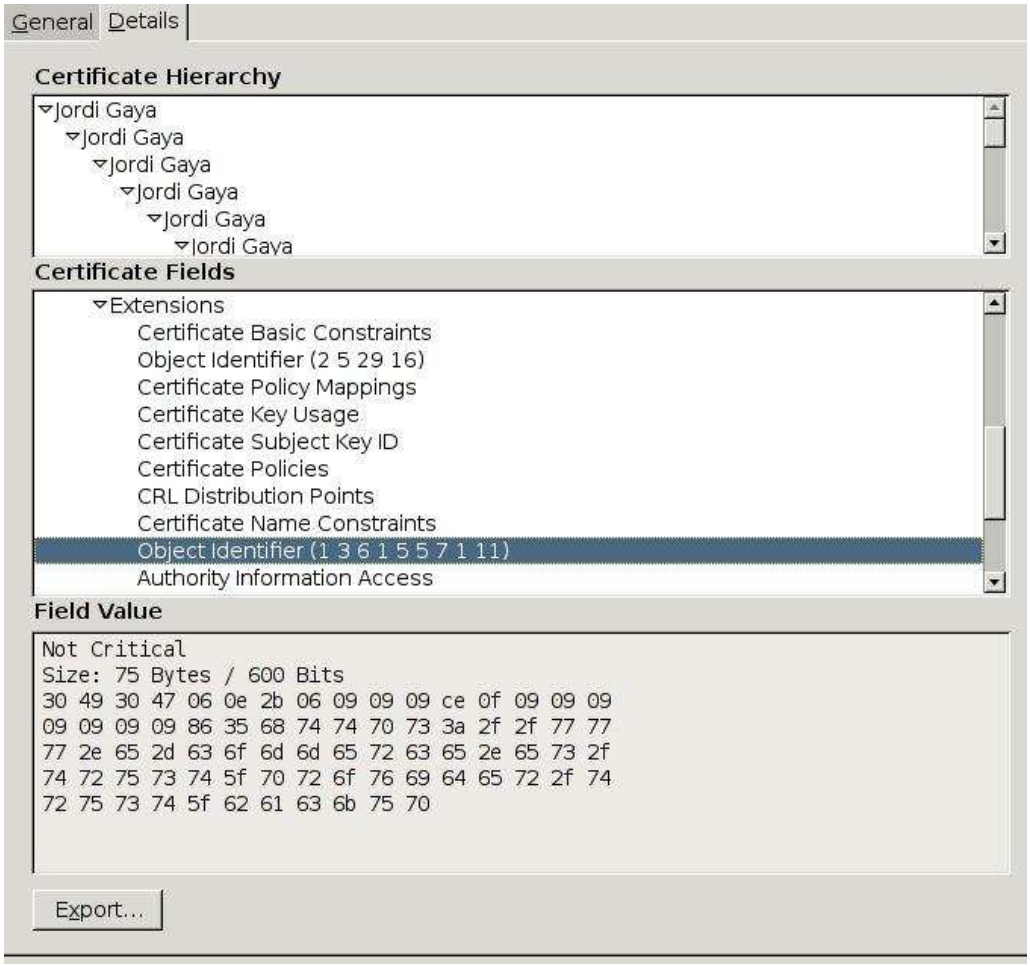

Figura 5.4: Mostra de l'extensió del certificat vista des del navegador

```
X509v3 extensions:
    X509v3 Basic Constraints: critical
        CA:TRUE, pathlen:1
    X509v3 Private Key Usage Period:
        Not Before: Sep  1 22:46:11 2009 GMT, Not After: Sep  1 22:46:11 2010 GMT
    X509v3 Policy Mappings:
        1.3.6.1.4.1.2706.2.2.1.1.1.1.1:1.3.6.1.4.1.2706.2.2.1.2.1.1.1
    X509v3 Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Certificate Sign, CRL Sign
    X509v3 Subject Key Identifier:
        01:02:03:04:05:06:07:08:09
    X509v3 Certificate Policies:
        Policy: 1.3.6.1.4.1.2706.2.2.1.1.1.1.1
          User Notice:
            Explicit Text: This certificate may be used for demonstration purposes only!

    X509v3 CRL Distribution Points:
        URI:http://jordi.gayas.crl/ec-ur.crl/test.crl
        reasons:<UNSUPPORTED>

    X509v3 Name Constraints:
        Permitted:
          email:*.deic.uab.cat

    Subject Information Access:
        1.3.6.9.9.9.9999.9.9.9.9.9.9.9 - URI:https://www.sports.fifa/trust_provider/trust

    Authority Information Access:
        unstructuredName - URI:http://testing.ca.com/ocsp

    X509v3 Policy Constraints:
        Require Explicit Policy:3, Inhibit Policy Mapping:7
    X509v3 Issuer Alternative Name:
        URI:http://www.ca_de_confian@a_edu.com/
    X509v3 Subject Alternative Name:
        IP Address:127.0.1.1
    X509v3 Authority Key Identifier:
        keyid:01:02:03:04:05:06:07:08:09
        URI:http://ca.test.com/
```

Figura 5.5: Output del OpenSSL on s'observa el contingut del camp amb OID 1.3.6.1.5.5.7.1.11

d'arbre eficient. Veure figures 4.2 i 4.3 on es mostren exemples de una llista de confiança i la llista de proveïdors de confiança respectivament. Un cop es disposa del certificats destinats per un sector específic, segons l'ontologia basada en sectors d'aplicació del diferents dominis de PKI, s'agruparan segons s'ha esmentat en una base de dades plana configurada amb un XML, on el tag que determina la temàtica del certificat serà la següent:

```
<List>
  <TrustProvider>
    <Name>CN=TrustProvider, O=Ministry of Business,C=USA </Name>
    <Context>Law</Context>
    <Scope> Spain</Scope>
    <CertProvider> OU= FNMT Clase 2 CA ,O=FNMT,C=USA </CertProvider>
    <Reference>https://www.e-commerce.es/trust_provider/trust</Reference>
  </TrustProvider>
   <TrustProvider>
    <Name>CN=TrustProvider, O=Ministry of education,C=USA </Name>
    <Context>E-Learning</Context>
    <Scope> Spain </Scope>
    <CertProvider> OU= FNMT Clase 2 CA ,O=FNMT,C=USA </CertProvider>
    <Reference>https://www.uoc.edu/trust_provider/trust</Reference>
  </TrustProvider>
   <TrustProvider>
    <Name>CN=TrustProvider, O=Ministry of Sports,C=ES </Name>
    <Context>Sports</Context>
    <Scope> Spain </Scope>
    <CertProvider> OU= FNMT Clase 2 CA ,O=FNMT,C=HN </CertProvider>
    <Reference>https://www.sports.fifa/trust_provider/trust</Reference>
  </TrustProvider>
</List>

</TrustList>
<CertList>
    <CA>
      <CertProperties>
        <Subject>CN=Autoritat de certificacio</Subject>
        <Issuer>CN=Jordi Gaya Sans</Issuer>
        <Validity>
          <NotBefore> </NotBefore>
```

```
            <NotAfter> </NotAfter>
          </Validity>
            <EncodedCert>dkasdjkada </EncodedCert>
        </CertProperties>
        <Constrains>
          <ProvidesSecurity/>
          <ApplicationContext/>
          <TrustLevel>8</TrustLevel>
          </Constrains>
          <URI>edu.crt</URI>
    </CA>
     <CA>
        <CertProperties>
          <Subject></Subject>
          <Issuer></Issuer>
          <Validity>
            <NotBefore></NotBefore>
            <NotAfter></NotAfter>
          </Validity>
            <EncodedCert></EncodedCert>
        </CertProperties>
        <Constrains>
          <ProvidesSecurity/>
          <ApplicationContext/>
          <TrustLevel>8</TrustLevel>
        </Constrains>
        <URI>edu_backup.crt</URI>
    </CA>
</CertList>
 </TrustList>
```

Per filtrar les cerques i poder extreure els certificats segons el sector d'aplicació s'utilitza la següent funció en el JS , amb el que es coneix com XML Path Language (XPath), segons es mostra a continuació

```
req.open("GET", "tp_list.xml", false);
req.send(null);
var xmlDoc = req.responseXML;
var nsResolver = xmlDoc.createNSResolver( xmlDoc.ownerDocument == null ? xmlDoc.documentElement
                                        : xmlDoc.ownerDocument.documentElement);
```

```
switch(this.TipusSeleccionat)
{
        case 0:path_dir ='/List/TrustProvider[1]/Reference';break;
        case 1:path_dir ='/List/TrustProvider[2]/Reference';break;
        case 2:path_dir ='/List/TrustProvider[3]/Reference';break;
}

        var nodes=xmlDoc.evaluate(path_dir, xmlDoc, null, XPathResult.ANY_TYPE, null);
        var result=nodes.iterateNext();
```

5.1.4 Integració dels mòduls

A grans trets, la integració dels mòduls s'ha realitzat en el següent ordre:

- **Pas 1**: Generació de l'extensió , TPL ens indica la ubicació de les CA confiables per un sector d'aplicació basat en una ontologia establerta.
- **Pas 2**: Generació de la base de dades amb XML per vincular totes les CA amb la seva ontologia associada.
- **Pas 3**: Implementació del *plugin* o extensió del navegador per realitzar la selecció de la temàtica i accés als TP.
- **Pas 4**: Finalment, ubicació dintre del *plugin*, exactament en *chrome://trustprovider/content/* la base de dades dels proveïdors de confiança, per gestionar i estendre la confiança per part del usuari amb les recomanacions del TP.

5.1.5 Problemes trobats

Alhora d'implementar l'enllaç del Proveïdor de Confiança TPL, com a extensió de la funcionalitat del certificat X.509v3 m'he trobat amb moltes dificultats a nivell de programació , ja en incidències i problemàtiques a nivell de dependències de les llibreries *IAIK*, com en el fet de generar una nova extensió amb un OID

únic. A grans trets, tota extensió recollida en l'estàndard X.509v3 té assignat un OID respectivament, per tant basant-nos en el fet de la comprovació OID , s'ha procedit a assignar el següent identificador *1.3.6.1.5.5.7.1.11* vinculat al *Subject Information Access* (veure 5.1).

Cas d'error amb OID no reconegut:
Extension 9: not critical 1.3.6.1.5.5.7.1.99
UnknownExtension: OBJECT ID = TrustProvidersLink
SEQUENCE[C] = 1 elements
Cas amb OID= 1.3.6.1.5.5.7.1.11
public static final ObjectID oid = new ObjectID("1.3.6.1.5.5.7.1.11", "TrustProvidersLink");
Extension 9: not critical TrustProvidersLink
accessMethod: OBJECT ID = TPL
accessLocation: uniformResourceIdentifier: https://www.uoc.edu/trust-provider/trust

Taula 5.1: Error amb els OID's (TPL)

5.2 Resum

En aquest capítol s'ha explicat com s'ha organitzat el codi a partir del disseny que s'ha realitzat del model explicat en el capítol de disseny. També s'han comentat amb detall les decisions d'implementació que s'han adoptat amb l'objectiu d'oferir el compliment dels requeriments i el bon funcionament del model.

Capítol 6

Proves

En aquest capítol s'explica l'entorn on s'han dut a terme els tests del model. Finalment s'analitza els resultats obtinguts i se'n fa una interpretació exhaustiva.

6.1 Introducció

Un cop realitzada la implementació del nou model de confiança basat en proveïdors de confiança, és moment de dur a terme els tests que verifiquin el seu correcte funcionament.

6.2 Entorn de Proves

Les proves de funcionament s'han realitzat en un ordinador personal amb sistema operatiu *Kubuntu* GNU/Linux. amb *Kernel 2.6.28-11-generic* i navegador web *Firefox* v.3.0.10.

6.3 Resultats

La presentació dels resultats es farà de manera seqüencial i s'anirà explicant el funcionament pas a pas de l'extensió.

- Pas 1: El navegador té 2 entrades per interaccionar amb el usuari, una en el menú (barra d'eines) i l'altra en la part inferior.
- Pas 2: Mirar el apartat opcions (veure 6.1 i selecciona segons es desitgi.
- Pas 3: Mirar en la finestra principal el botó informació que ens mostrara el funcionament del plugin en unes senzilles passes.(Veure Figura 6.2)
- Pas 4: Posteriorment, seleccionar un context d'aplicació del certificat (Veure Figura 6.3)
- Pas 5: Una vegada elegit,se'ns mostrarà les CA's disponibles per descarregar.(Veure Figura 6.4)
- Pas 6: Es guarda el *.crt corresponent i es pregunta si es desitja procedir a la instal·lació.(Veure Figura 6.5)
- Pas 7: Es procedeix a la instal·lació (veure Figura 6.8) o es mostra una finestra informativa segons l'elecció feta prèviament pel usuari.(Veure Figura 6.7)

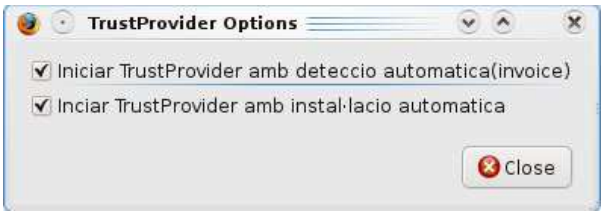

Figura 6.1: Finestra d'opcions de configuració

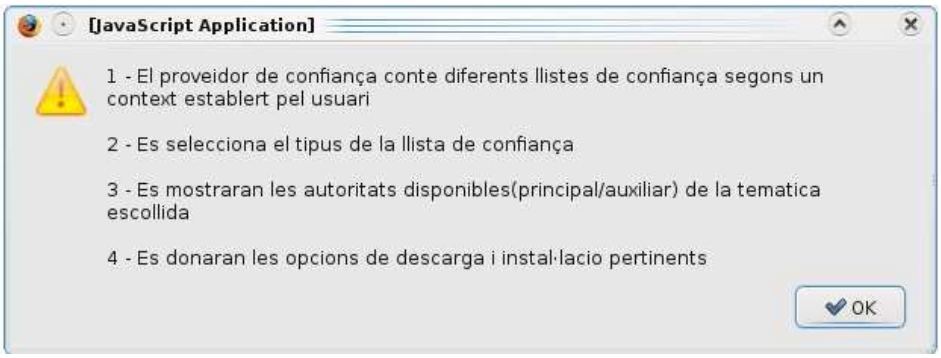

Figura 6.2: Quadre informatiu inicial de les passes a seguir

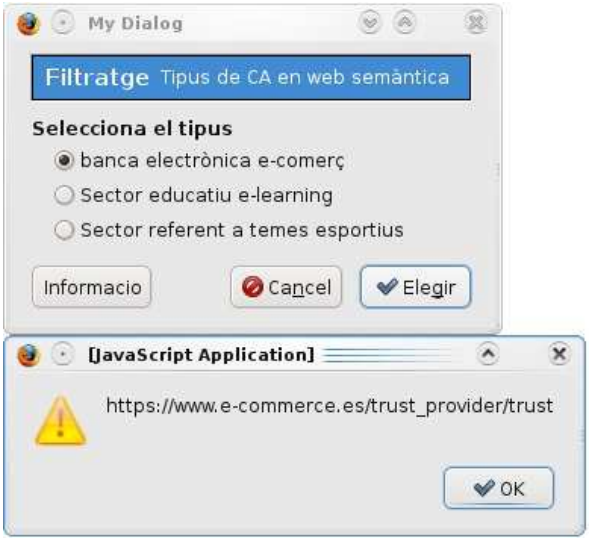

Figura 6.3: Finestra per seleccionar el context d'aplicació del certificat i el TPL respectiu

Figura 6.4: Elecció entre CAs disponibles

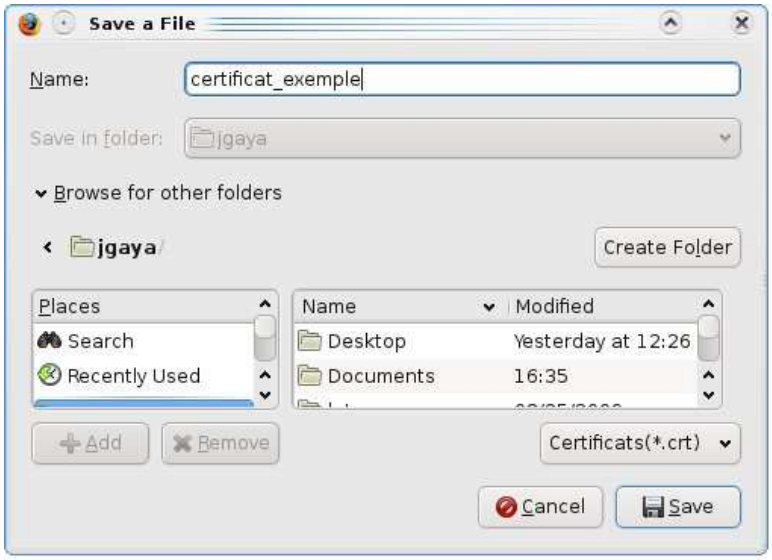

Figura 6.5: Finestra per descarregar el certificat *.crt

Figura 6.6: Diàleg de confirmació per realitzar la instal·lació

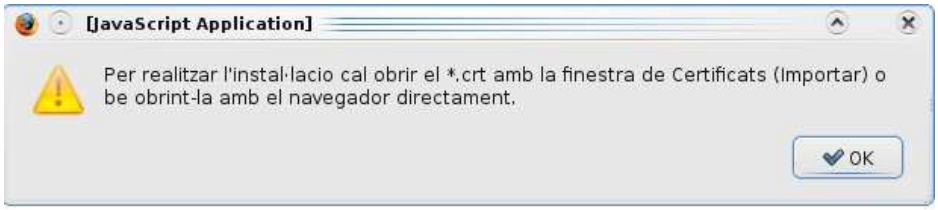

Figura 6.7: Quadre informatiu com realitzar la instal·lació

Figura 6.8: Finestra d'instal·lació del certificat

6.4 Resum

En aquest capítol s'han explicat els tests que s'han dut a terme per al nou model de confiança. Primer s'ha descrit l'entorn de proves on s'han executat els tests. Finalment s'han comentat i raonat els resultats obtinguts. A partir d'aquests resultats s'han pogut extreure conclusions que s'explicaran en el següent capítol.

Capítol 7

Conclusions

En aquest capítol es resumeix la feina feta i s'enumeren els objectius assolits. Posteriorment s'expliquen les conclusions a les què s'ha arribat en base als resultats obtinguts i es presenten una sèrie de línies de treball. Finalment es fa una valoració personal del projecte.

Els problemes d'interoperabilitat entre dominis de PKI són un dels principals problemes que s'han resoldre per tal de permetre un desplegament massiu de la tecnologia PKI. Tot i que les diverses solucions s'han proposat fins ara, cap d'ells té èxit en el mercat a causa de restriccions tècniques, polítiques i socials. En aquest treball s'ha presentat un nou model de desenvolupament de la confiança més flexible que els anteriors des del punt de vista de l'usuari. El model proposat es basa en llistes de confiança per tal de resoldre els problemes d'interoperabilitat entre dominis de PKI.Aquesta proposta es basa en un model jeràrquic de PKI i s'estén la confiança mitjançant uns proveïdors de confiança. Com hem vist en el Model de BVA, l'entitat de confiança no és una CA, es un TP en el nostre cas. L'ús de TPs faciliten l'adopció dels interdominis de CA pels usuaris, perquè són les entitats més properes en les quals els usuaris realment coneixen i hi tracten. Els TPs han guanyat la seva reputació en una determinada comunitat pel seu bon

funcionament i són de confiança en la seva àrea d'especialització. Els TPs són utilitzats per donar recomanacions, ajudar els usuaris a interpretar les polítiques de seguretat de les CAs i donar-lis-hi informació sobre els dominis de PKI. D'altra banda, la promoció i difusió dels TPs s'aconsegueix gràcies a un nova extensió del certificat que ofereix informació de les entitats que recolzen el seu domini de PKI. Tanmateix, l'arquitectura presentada ofereix una classificació de les llistes de confiança expressades en un llenguatge semàntic, el qual ofereix un enfocament més específic sobre quan es pot afirmar si es adequat o no d'acceptar un certificat. L'ús d'ontologies és doble: en primer lloc permet descriure les complexes relacions del món real en una llengua que és interpretable per les computadores i en segon lloc, ens proporciona la base per implementar interfícies amb llenguatge natural per als TP, de manera que les aplicacions puguin ser desenvolupades fàcilment i d'ús general, encara que no es tinguin els coneixements tècnics suficients.

7.1 Assoliment d'Objectius

En aquest apartat s'enumeraran els objectius assolits relacionant-los amb els objectius inicialment plantejats en el capítol d'introducció.

1. S'ha assolit satisfactòriament la implementació d'un model basat en proveïdors de confiança,amb ús d'ontologies per classificar els atributs de confiança.

2. S'ha assolit satisfactòriament l'anàlisi dels requisits que ha de tenir el nou model que es desenvoluparà.

3. S'ha assolit satisfactòriament la implementació de l'extensió de funcionalitat en certificats X.509v3 i la garantia de compatibilitat amb les aplicacions actuals.

4. S'ha assolit satisfactòriament el disseny i la construcció d'un joc de proves que ha permés avaluar el funcionament i rendiment del nou model.

7.2 Conclusions dels Resultats Obtinguts

Els resultats (veure secció 6.3) mostren un funcionament òptim del model, assolint tots els requisits (veure 3.1) establerts prèviament en l'anàlisis del model.

7.3 Línies de Millora i Treball Futur

En aquest apartat comentarem aquelles línies en les que es podria aprofundir per tal de millorar el model de confiança presentat en aquest projecte. Aquestes línies de millora es basen en vies d'investigació es centraran en la definició d'ontologies específiques per els gestors de la llista de confiança per permetre una gestió altament configurable i automàtica de les llistes de l'usuari.

7.4 Valoració Personal del Projecte

Aquest projecte m'ha aportat una experiència personal molt gratificant i enriquidora, on he anat consolidant un projecte de final de carrera, de principi a fi, amb totes les seves incidències i contratemps a mesura que s'ha anat avançant en cada una de les parts,on s'ha realitzat una segmentació del model en diversos mòduls per tractar de resoldre el problema per parts, aplicant l'estratègia de programació *divideix i guanyaràs*.

La metodologia d'elaboració de projectes que se'm van instruir des del departament d'Enginyeria de la Informació i de les Comunicacions (dEIC), ha sigut d'una gran ajuda per realitzar una correcta planificació i no perdre la visió general

del problema. Identificant les fites i requeriments necessaris per completar amb èxit el projecte, fent un acompliment dels objectius establerts prèviament. Aquest procés m'ha permès planificar, gestionar ,implementar i valorar objectivament un treball tècnic de gran magnitud ,pas que m'ha ajudat a realitzar-me com a enginyer i ha tindre una visió general dels problemes i saber-los tractar amb ús de metodologies.

Declaració de les Fonts

Aquest projecte ha estat basat en l'article [PKIInterdomain], el qual ha sigut la pedra angular del projecte, com a referent de consulta i com a font d'informació incondicional per la realització del anàlisis, disseny i implementació del model. Tantmateix, cal esmentar l'us gràfic de les imatges incorporades per realitzar l'estat de l'art del projecte, han estat extretes de les següents direccions web , sense restriccions d'ús i difusió per part de l'autor, veure cites [url1],[url2],[url3],[url4]

Bibliografia

[NetCon] Casola, V., Mazzeo, A., Mazzocca, N., Vittorini, V.: Policy Formalization to combine separate systems into larger connected network of trust. In: Proc. of Int. Conf. on Network Control and Engineering for QoS, Security and Mobility (Net-Con)(2002)

[RFC3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S.: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. IETF RFC 3647 Informational (2003)

[EuroPKI2005] Casola, V., Mazzeo, A., Mazzocca, N., Rak, M.: An Innovative Policy-Based Cross Certification Methodology for Public Key Infrastructures. In: Chadwick, D., Zhao, G. (eds.) EuroPKI 2005. LNCS, vol. 3545, pp. 100–117. Springer, Heidelberg (2005)

[RFC4158] Cooper, M., Dzambasow, Y., Hesse, P., Joseph, S., Nicholas, R.: Internet X.509 Public Key Infrastructure: Certification Path Building. IETF RFC 4158. Informational(2005)

[RFC3280] Housley, R. , Polk, W. , Ford, W. ,Solo, D. ,:Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. IETF RFC 3280.(April 2002)

[XPath] Berglund, A., Boag, S., Chamberlin, D., Fernndez, M.F., Kay, M., Robie, J., Simon,J.: XML Path Language (XPath) 2.0. W3C Recommendation (2007)

[ETSI] ETSI: Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust Service Provider status information. Draft ETSI TS 102 231 V1.2.1 (2005)

[Ontology] Bechhofer, S., van Harmelen, F., Hendler, J., Horrocks, I., McGuinness, D.L., Patel-Schneider, P.F., Stein, L.A.: OWLWeb Ontology Language.W3C Recommendation (2004)

[ECMAScript] Standard ECMA-262 2nd Edition - August 1998

[PKIInterdomain] Rifa-Pous, H., Joancomartí-Herrera , J. : An Interdomain PKI Model Based on Trust Lists, 4th European PKI Workshop: Theory and Practice, (EuroPKI), LNCS, Volume 4582, pp. 49–64, 2007

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C. :X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP ,The Internet Society (June 1999)

[RFC3161] Adams, C., Cain, P., Pinkas, D., Zuccherato, R. :RFC3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) ,The Internet Society (August 2001)

[RFC2510] Adams, C., Farrell, S. : Internet X.509 Public Key Infrastructure Certificate Management Protocols, The Internet Society (March 1999)

[Stallings] Stallings, W., Mecklermedia's official Internet world Internet security handbook,IDG Books, San Mateo, CA USA 1995

[JCE-IAIK] iaik.x509 Class V3Extension ,IAIK-JCE 3.13, (c) 2002 IAIK, (c) 2003 SIC, http://javadoc.iaik.tugraz.at/iaik-jce/3.13/iaik/x509/V3Extension.html

[url1] :3-PKI Architectures , Networking government in New Zealand, E-governement Programe, http://www.e.govt.nz/archive/services/see/see-pki-paper-4/chapter3.html

[url2] Masaki Shimaoka , Standardization of multi-domain PKI interoperability , Authentication Platform Group http://www.secom.co.jp/isl/e2/research/cs/report01/

[url3] Soluciones de comercio electrónico ,CIPRES-UPM. Enero 1999.:http://greco.dit.upm.es/ enrique/ce/sec2/par211.html

[url4] Montero, Victor H., Meiners, Leandro F.,: Interoperablidad en PKI,http://www-2.dc.uba.ar/materias/.../Informe-Interoperabilidad-PKI-v3.pdf

Firmat: Jordi Gaya Sans

Bellaterra, setembre de 2009

Resum

En aquest projecte s'ha presentat un nou model de desenvolupament de la confiança, més flexible que els anteriors, des del punt de vista de l'usuari. El model proposat es basa en llistes de confiança per tal de resoldre els problemes d'interoperabilitat entre dominis de PKI. Aquesta proposta es basa en un model jeràrquic de PKI on s'estén la confiança mitjançant uns proveïdors de confiança.

Resumen

En este proyecto se ha presentado un nuevo modelo de desarollo de la confianza, más flexible que los anteriores, según el punto de vista del usuario. El modelo propuesto se basa en listas de confianza para resolver los problemas de interoperatividad entre dominios de PKI. Esta propuesta se basa en un modelo jerárquico de PKI donde se extiende la confianza gracias a unos proveedores de confianza.

Abstract

The current project manifests a new model for the development of the trust, thus being more flexible that the previous models, as the users have qualified it. The proposed model is based on trust lists in order to resolve interoperability issues of interdomain PKIs. It is built upon a hierarchical PKI model and extends trust using TPs.